SIEMENS

Siemens Remote Service

CS

Troubleshooting Guide

System

Siemens Remote Service

© Siemens 2007
The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Print No.: TDIT-SRS.840.01.02.02
Replaces: TDIT-SRS.840.01.01.02

English
Doc. Gen. Date: 03.08

Document revision level

The document corresponds to the version/revision level effective at the time of system delivery. Revisions to hardcopy documentation are not automatically distributed.

Please contact your local Siemens office to order current revision levels.

Disclaimer

The installation and service of equipment described herein is to be performed by qualified personnel who are employed by Siemens or one of its affiliates or who are otherwise authorized by Siemens or one of its affiliates to provide such services.

Assemblers and other persons who are not employed by or otherwise directly affiliated with or authorized by Siemens or one of its affiliates are directed to contact one of the local offices of Siemens or one of its affiliates before attempting installation or service procedures.

Table of Contents 3

1 General Information 6

Requirements . . . 6
Required Test Equipment, Tools and Aids . . . 6
Notes . . . 7
General Safety Information . . . 7
Screenshots & Graphics in this Document . . . 7
Abbreviations . . . 8

2 Information Regarding Network Configuration 9

Network Types . . . 9
Medical System and SRS Router in the same Network, without Customer Gateway 9
Medical System and SRS Router in the same Network, with Customer Gateway . . 10
Medical System and SRS Router in Different Network Areas . . . 11
VPN, Virtual Private Network . . . 12

3 Connectivity 13

Site Identification . . . 13
IP Address . . . 15
Changing the IP Address . . . 16
Static Routes . . . 18
Adding / Checking Routes to the SIEMENS Remote Service Router . . . 18
Network Address Translation (NAT) . . . 20
Outside NAT . . . 20
Inside NAT . . . 21
Connectivity Test . . . 22
Prerequisites . . . 22
Procedure . . . 22
Example: IP connection to the SRS server does not work . . . 25
Test Ping not Alive . . . 29
Handling the Pre-Connect Tool . . . 31
Checking all Prerequisites . . . 31
Test Procedure . . . 32
Reactive Remote Service via CORINA . . . 38
Problems with Remote Service via CORINA . . . 38

4 SRS Functionalities 40

Basic Ports . . . 40
From the Customer System (Modality) to Siemens (DMZ) . . . 40
From Siemens (DMZ) to the Customer System (Modality) . . . 40
FTP . . . 41
RDIAG Server (FTP Target Server) . . . 41
Password . . . 41
FTP Test Transfer . . . 41
Syngo Auto Transfer List . . . 43
Deleting the Transfer List . . . 43

File & Image Transfer does not work . . . 44
Mail . . . 47
RDIAG Server . . . 47
Mail Test . . . 47

5 System Management (MNP) 50

MNP Installation/Activation of VExx and VFxx Versions . . . 50
MNP Registration Procedure . . . 50
MNP Installation/Activation of VGxx Versions . . . 52
MNP Registration Procedure . . . 52
TCP/IP Ports . . . 54
From the Customer System (Modality) to Siemens (DMZ) . . . 54
From Siemens (DMZ) to the Customer System (Modality) . . . 55
Troubleshooting System Management . . . 57
Log Files . . . 57
Description of the Log File, including Corrective Action . . . 57
General Information regarding System Management . . . 64
System Management Installation Check . . . 66
System Management Connectivity Check . . . 67

6 Remote Update Handling (RUH) 69

Remote Update Handling / Software Distribution . . . 69

7 Virus Protection 70

Virus Protection . . . 70
Prerequisites . . . 70
Downloading the latest Pattern Files . . . 71
Checking the Functionality of Software Distribution of the Virus Pattern (silent mode) . 74

8 Additional Information 76

Help Desk . . . 76
SRS Toolkit . . . 77
Final Configuration Checklist . . . 77
Router Order Form . . . 77
Pre-Connect Tool (download) . . . 77
Siemens Remote Portal Access . . . 78
Knowledge Base / Life Net . . . 79
Prerequisites . . . 79
Accessing the CS Knowledge Base for Systems without syngo or syngo lower than VE31C . . . 81
Accessing the CS Knowledge Base from syngo VE31C onwards . . . 83
Login to the CS Knowledge Base . . . 86
Passwords . . . 88
Passwords in the CS Knowledge Base . . . 88
SRS Access Server . . . 89
System Management Server . . . 90

SRS Backend for MNP Versions VExx and VFxx 90
SRS Backend for MNP Version VGxx 90
Country Codes 92

9 Changes to Previous Version 96

10 Index 97

Requirements

Required Test Equipment, Tools and Aids

Pre-Connect Tool

The Pre-Connect Tool (PCT) allows/helps you to test the SRS capability in the customer's networks. The tool tests SRS network connectivity on the port level for your system type. The tool has to be installed on the service laptop.

Refer to `Siemens MED Intranet > For Service > Product information > Siemens Remote Service > CB-DOC > Installation > System > Installation Instructions`

The tool and the documents **Pre-Connect Tool Setup Software** and **Pre-Connect Tool Vxxxx Installation Instructions** can be found there.

Notes

General Safety Information

When performing the work steps and checks, the general safety information for medical products must be observed.

Screenshots & Graphics in this Document

Screenshots and graphics used in this document should be viewed as examples only.

They cannot describe all possible input combinations; they have an informative character and are used only for better orientation.

The actual parameters that must be configured can be found in the text and the tables, or depend on the requirements and configuration (items included in the shipment) of the individual system.

Abbreviations

SRS portal	Siemens Remote Service portal
RDiag portal	old wording for SRS portal
RDiag	Remote Diagnostics
RUH	Remote Update Handling
MNP	Managed Node Package
NAT	Network Address Translation
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
UDP	User Datagram Protocol
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
HTTPS	Hypertext Transfer Protocol Secure
LAN	Local Area Network
VPN	Virtual Private Network
SMTP	Simple Mail Transfer Protocol
IP Sec	Internet Protocol Security
SW	Software

Network Types

Examples for the SRS Gateway Configuration

Medical System and SRS Router in the same Network, without Customer Gateway

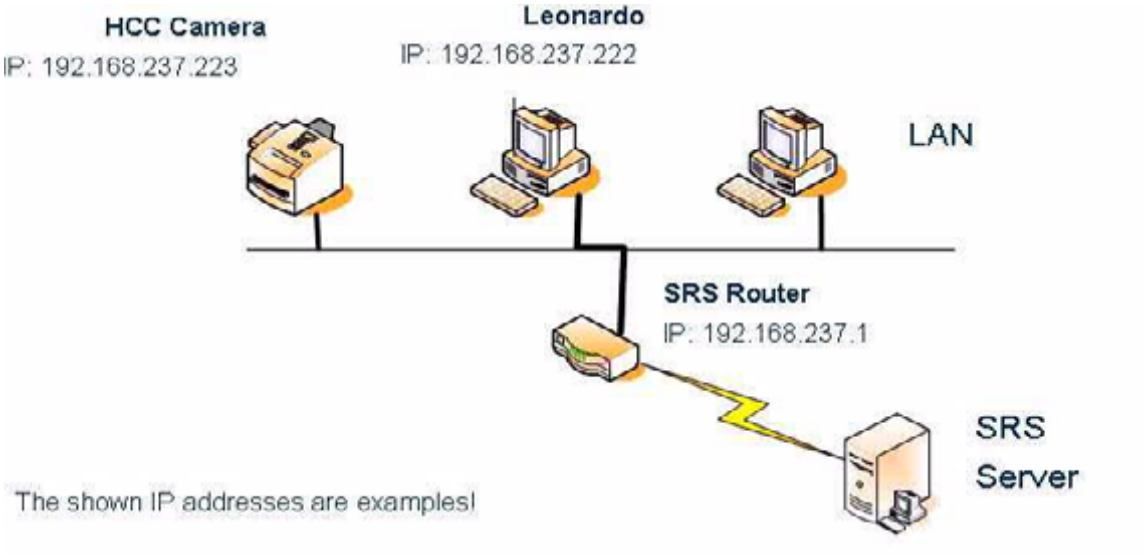

Fig. 1: SRS Router in same network

Only recommended possibility:

- Enter the SRS router as the **Gateway** in the medical system configuration of “Local Host”. For system-specific entries, refer to the corresponding configuration guide.

Medical System and SRS Router in the same Network, with Customer Gateway

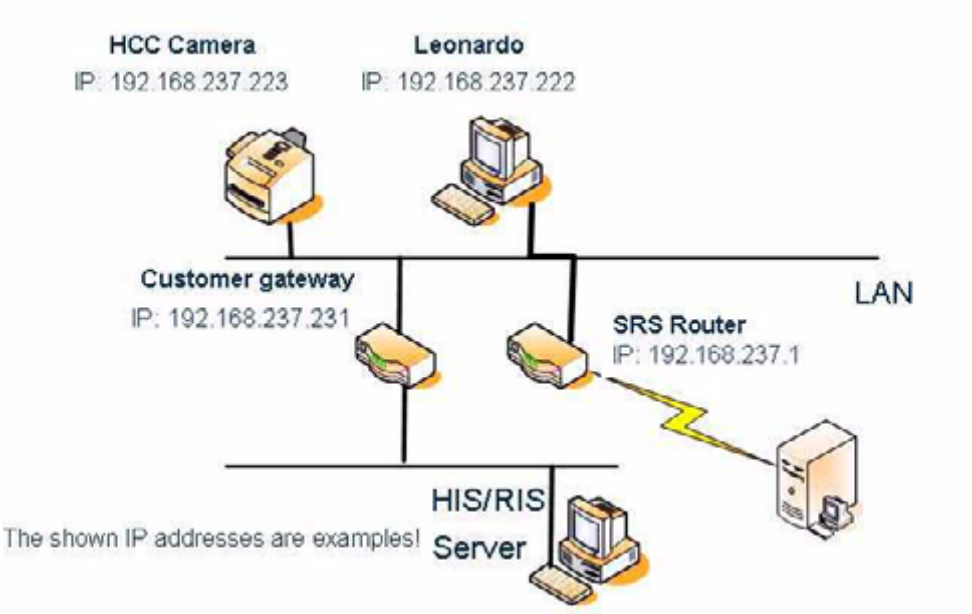

Fig. 2: SRS Router in same network with gateway

Recommendation:

- **Possibility 1,** because this always ensures that the customer's network functions will function again after proper and complete loading of the medical system software.
  - **Alternative: Possibility 2.**

Possibility 1:

1. **With** the involvement of the hospital's network administrator.
2. Enter the customer's gateway into the medical system as the **"Default Gateway"**.
   - The customer's "local Gateway" is included in the medical system data backup "backup & restore" and is restored when the software is downloaded.
3. **Configure the**SRS router **in the customer's** "local Gateway".

   This must be carried out by the network administrator of the customer. The customer's local gateway automatically transfers desired communication between the medical system and the SRS server or from the SRS server to the medical system via the SRS router.
   - The Setup Data of the local gateway are saved by the customer (Data Backup) and any SW download of the customer's local gateway is again "restored".

Possibility 2:

1. **Without** the involvement of the hospital's network administrator.
2. Enter the customer's gateway into the medical system as the **"Default Gateway"**.
   - The customer's "local Gateway" is included in the medical system data backup "backup & restore" and is restored when the software is downloaded.

3. Enter **the** IP address of the SRS router **in** the medical system as **“static route”**.(Static Routes / p. 18)
   - The customer's “local Gateway” is included in the medical system data backup “backup & restore” and is restored when the software is downloaded.

Medical System and SRS Router in Different Network Areas

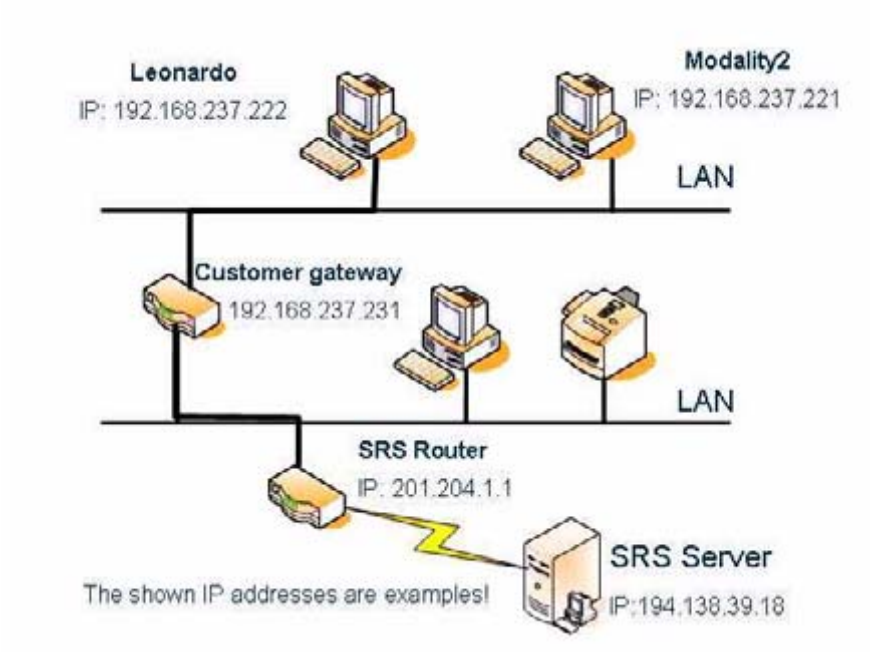

Fig. 3: SRS Router in different network area

Only recommended possibility:

1. **With** the involvement of the hospital's network administrator.
2. Enter the **local/customer gateway** as (the) "**Default Gateway**" into the configuration of the medical system. .
   - The customer's “local Gateway” is included in the medical system data backup “backup & restore” and is restored when the software is downloaded.
3. **Configure the** SRS router **in the customer's** “local Gateway”.

   This must be carried out by the network administrator of the customer. Then the local gateway of the customer is able to transfer packets of the communication between the medical system and the SRS server.
   - The Setup Data of the local gateway are saved by the customer (Data Backup) and any SW download of the customer's local gateway is again “restored”.

VPN, Virtual Private Network

VPN stands for **V**irtual **P**rivate **N**etwork.

For this, an IP Sec tunnel is set up between the SRS server and the VPN end point at the customer's location.

The beginning and end of this "tunnel" are determined by what are called "Internet security end points".

The VPN configuration is carried out between the hospital's network administrator and the SRS Help Desk (Help Desk / p. 76).

The network administrator defines the hospital routing and makes the "default gateway" available that is used by the medical system to reach the "Internet security end point".

This gateway must be configured in the medical system.

The SRS Helpdesk enters the configuration parameters at the SRS server and checks the connection.

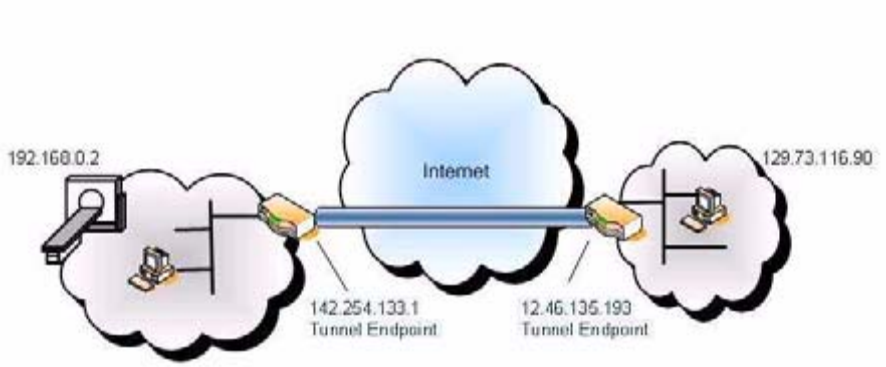

Fig. 4: VPN tunnel

Site Identification

During initial startup, the “**Computer name**“ must be reassigned under “Identification“.

Computer name

- The **computer name** (= **host name**) may be entered only in capital letters. It may include up to 14 characters. The characters "_" and "-" should be avoided, as they could cause problems (even though it is possible to enter them).

  The computer name may not consist of only numeric characters and may not start with a numeric character.

- **Computer Name Restrictions:**
  - **it must be done in agreement with the local network administrator!**
  - **It must be unique in the network!**
  - **Only capital letters may be used!**
  - **Enter 1 to 14 characters**
  - **Do not use special characters** ; : " < > * + = \ | ? ,
  - **The characters“ _“ (underscore) and “-“ (minus) should be avoided, as they could cause problems (even though it is possible to enter them).**
  - **Do not use only numeric characters**
  - **Do not use numeric characters at the beginning of the name.**

- **Subsequently Changing the Computer Name**

  This has an effect on the Dicom AEs, the **Versant Database**, **System Management** as well as the **User Default Password !**

  a) **Prior to changing the computer and station names:**

  - Make sure that the patient images have been saved by the customer (archived) or save the patient images.
  - Read out the Dicom AEs and make a note of them.
  - Uninstall the System Management Base.

  b) **Changing the Computer and Station Names:**

  Change the computer name and station name and save them. The local AET is generated automatically from the computer name. Changing the computer name generates a pop-up window that allows you to select whether the AET should be changed as well. As soon as the DICOM connections are configured, the original AET should be kept.

  If the system message “`The computername has changed`...” is confirmed with **OK**, the AE titles will be overwritten. If **Cancel** is clicked on, the AETs will not be overwritten.

c) **After Changing the Computer and Station Names:**

- Immediately after changing the name, completely shut down the system and reboot it.
- Check the Dicom AETs and, if necessary, reenter the original AETs.
- Reinstall the System Management .
- Perform a new backup of the system data.
- Make the old backup of system data unusable.
- If wished, change the modified password that now automatically goes to "**User Given Password**" back to "**User Default Password** "!
- If the customer requests it, download the images that were saved and that the customer needs (Restore from Archive).

IP Address

NOTE

If DHCP is requested by the customer, make sure that the assigned IP address never expires (static DHCP), otherwise the system will not be able to access the Siemens Remote Server and will not be able to be accessed by Remote Service.

In order to do so, the Administrator needs to know the MAC address of the network interface card or of the network interface connected to the hospital network.

- **DHCP lease check**
  - Open a command shell
  - Enter: **ipconfig /all**

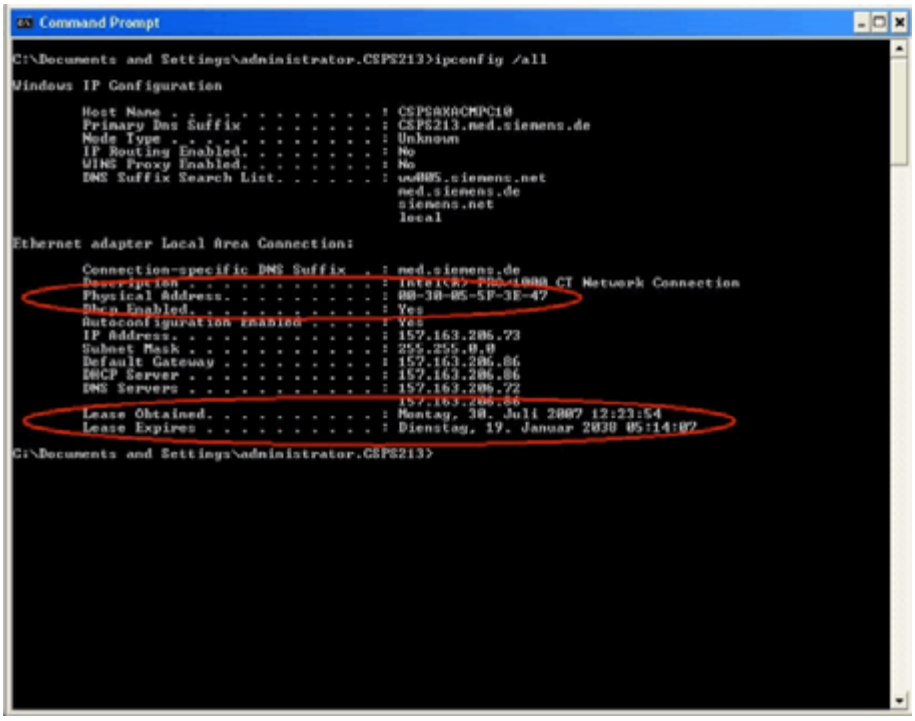
Command Prompt
C:\Documents and Settings\administrator.CSPS213>ipconfig /all
Windows IP Configuration
Host Name . . . . . : CSPSAXACMPC10
Primary Dns Suffix . . . . . : CSPS213.med.siemens.de
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : uwBB5.siemens.net
med.siemens.de
siemens.net
local
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : med.siemens.de
Description . . . . . : Intel(R) PRO/1000 CT Network Connection
Physical Address. . . . . : 00-30-05-5F-3E-47
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 157.163.206.73
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 157.163.206.86
DHCP Server . . . . . : 157.163.206.86
DNS Servers . . . . . : 157.163.206.72
157.163.206.86
Lease Obtained. . . . . : Montag, 30. Juli 2007 12:23:54
Lease Expires . . . . . : Dienstag, 19. Januar 2038 05:14:07
C:\Documents and Settings\administrator.CSPS213>

Fig. 5: IP Config with DHCP

Pos. 1 Physical Address

Pos. 2 Lease Obtained / Lease Expired

  - Write down the MAC address (physical address) (1/Fig. 5 / p. 15) and check the lease date (2/Fig. 5 / p. 15).

- **Specify an IP address**

  Usually this option is selected. The following three input boxes are then displayed:
  - **IP address**
  - **Subnet mask**
  - **gateways**

NOTE

If Specify an IP address (default) is deselected and Obtain an IP address from DHCP server is to be selected instead, first the entry for Default Gateway must be deleted with del.

NOTE

When entering the IP address, subnet mask or gateway address, a “0“ may not be at the beginning of any of the four three-digit numeric groups:

Correct: 221. 45. 1. 1 / Incorrect: 221.045.001.01

Effect of an incorrect entry: No “MedCom pending“ and a reboot when exiting the Service Software via Home. With the next bootup, the application software can no longer be downloaded completely and initialized.

Action to correct the error:

1. **Boot up the system as far as possible**
2. **Start the Service Software**
3. **Delete the inadmissible IP address with del**
4. **Enter the correct IP address and accept it with add**

NOTE

If the IP address 192.xxx.x.x already exists (default from the factory or from the software CD), it must be deleted.

Changing the IP Address

NOTE

Prior to changing the IP address, inform the SRS Help Desk (Help Desk / p. 76) about the change in the IP address so that the necessary changes to the SRS servers and firewalls can be made.

Otherwise the system will no longer be available for Remote Service and reinstallation of the System Management will fail.

The IP address must be changed with (e.g.):

Process	Reason
System Startup at the Customer's Site	When shipped, the IP address is entered by the production line.

Process	Reason
System Software Installation	When the system software is installed (TCP/IP LAN is not restored!), the default IP address from the software CD is already entered here.
Converting the Customer Network	When the customer reorganizes his network and assigns new IP addresses.

Changing the IP Address with System Management installed

1. Check whether System Management is installed and running.
2. Check which MNP version is being used by using the cmd **sysmgmt_install.exe -c**. For details, see Connectivity Test (Prerequisites / p. 22)
3. for MNP version VGxx (until May 2008).

   Call the SRS Help Desk and inform them.

   They or Engineering will update the **Synchronization file** between cRSP and the System Management Backend

   If this is not done, the reinstallation will fail! After May 2008, this is no longer necessary because a backend solution will then be implemented.
4. Disable the **Installed** and **Activated** checkboxes in the **Configuration** menu to uninstall System Management.
5. Change the IP address.
6. Reinstall System Management.

Static Routes

To make it possible for the IP package from one station (source/medical system) to reach another station (its destination/Siemens Remote Portal), the path to the destination must be known by all participating network components.

This information can be entered into a router with a static route.

Static routes are administratively defined routes that point to the next router (Hop) on the way to the destination network. Each router always send the packages to the next link in the chain using its routing table until the package finally reaches its destination.

Adding / Checking Routes to the SIEMENS Remote Service Router

To do this, they must be read out of the “Routing Table” and written down.

Checking the static route

- Open the service software (syngo)
- Select Utilities
- Select **Escape to OS** under source
- Type in **<route print>** in the Parameters box and press **Enter** ↵.

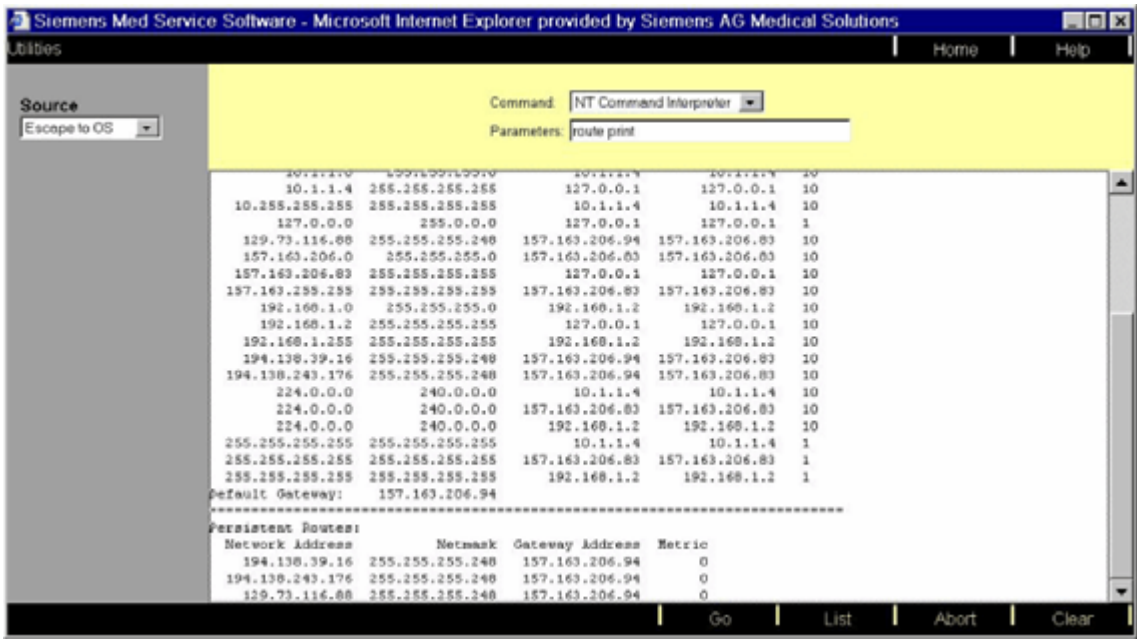

Fig. 6: Read out Persistent Routes with fallback Routes

Deleting an incorrect static route

- If you have an incorrect route, use the following command to delete it: .
  - route delete xx.xx.xx.xx (enter the IP of the "Network Address")

  e.g. for Europe (LUX09505 with IP 194.138.39.18)

  route delete 194.138.39.16 (or what is configured (Fig. 6 / p. 18))

Adding a static route

- Europe, Africa:
  route add -p 194.138.39.16 mask 255.255.255.248 xx.xx.xx.xx
- North / South America:
  route add -p 129.73.116.88 mask 255.255.255.248 xx.xx.xx.xx
- Asia:
  route add -p 194.138.243.176 mask 255.255.255.248 xx.xx.xx.xx

Replace the xx.xx.xx.xx with your customer router / gateway IP address!)

“-p“ means set persistent static route.

NOTE

You have to configure the static routes to all Remote Service Centers for every system. This provides the fallback concept for the remote diagnostics.

With Syngo VE31C or higher, this configuration is done automatically.

Network Address Translation (NAT)

Outside NAT

NOTE	**Outside NAT also can be called: Server NAT, Manager NAT or Destination NAT**

Outside NAT means the customer defines certain IP addresses that are used by the medical system to communicate with the Siemens environment (e.g. SRS access server). If the customer uses this function, the NAT addresses have to be configured in the Routing Tab card and System Management settings; otherwise, SRS will not work.

To determine whether there is an outside NAT

Outside NAT requires major changes to the SRS configuration that start in the router configuration. It therefore should be communicated to the CSE prior to performing the SRS configuration.

If outside NAT is used, please contact the SRS Help Desk (Help Desk / p. 76) for clarification and configuration of the SRS environment.

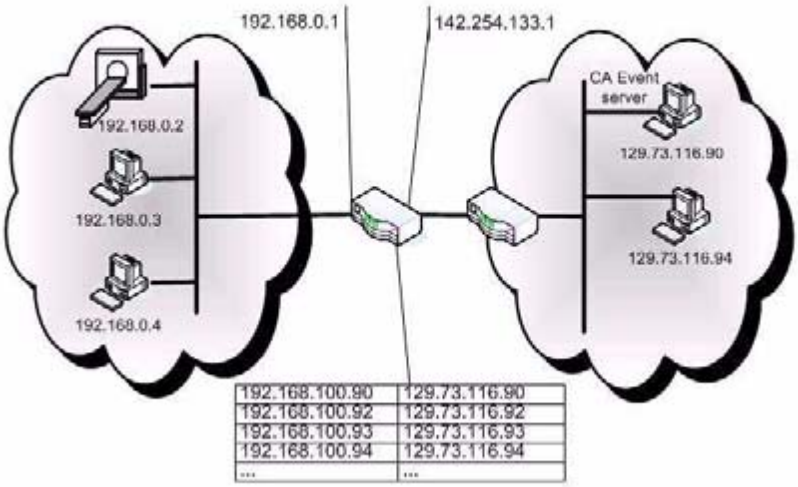

Fig. 7: Outside NAT

Inside NAT

NOTE	**Inside NAT can be also called: Local host NAT or Source NAT**

Inside NAT is required primarily when the customer address is already being used by another customer on the SRS server (duplicate addresses are not allowed on the SRS server).

In most cases, Inside NAT is implemented in the SRS router. The IP address of the system remains unchanged in the customer network; if the system data are sent over the SRS router, the IP address is translated.

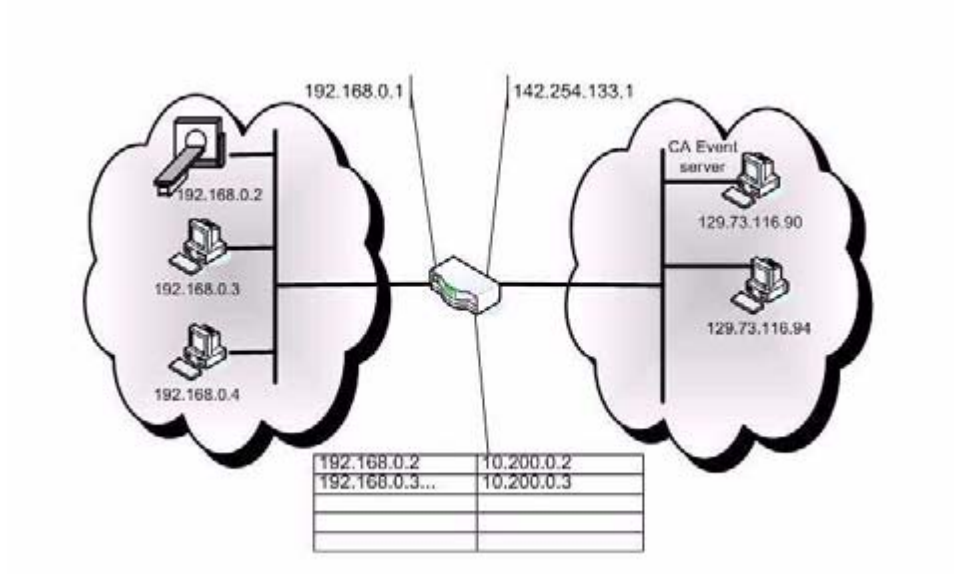

Fig. 8: Inside NAT

Connectivity Test

This test checks whether the connection from the medical system to the SRS server and to the System Management server is working.

Using the **“tracert”** command on the command level, the **“Ping”** signal path can be traced.

NOTE	**In some network configurations it is possible that the “Internet Control Message Protocol” will be blocked. In such cases, the “Ping” does not work. In this case, perform a connection test (Test Ping not Alive / p. 29) with the telnet command on the corresponding server. If this test also fails, the SRS Help Desk (Help Desk / p. 76) has to be contacted immediately.**

NOTE	**Outside NAT may be configured in the customer network.**

Prerequisites

- Installation and configuration of the router are completed
- The “Default Gateway” to the SRS router was configured in the medical system.
- Find out which MNP version is used by using the command sysmgmt_install.exe -c in %MEDHOME\service\mwtools

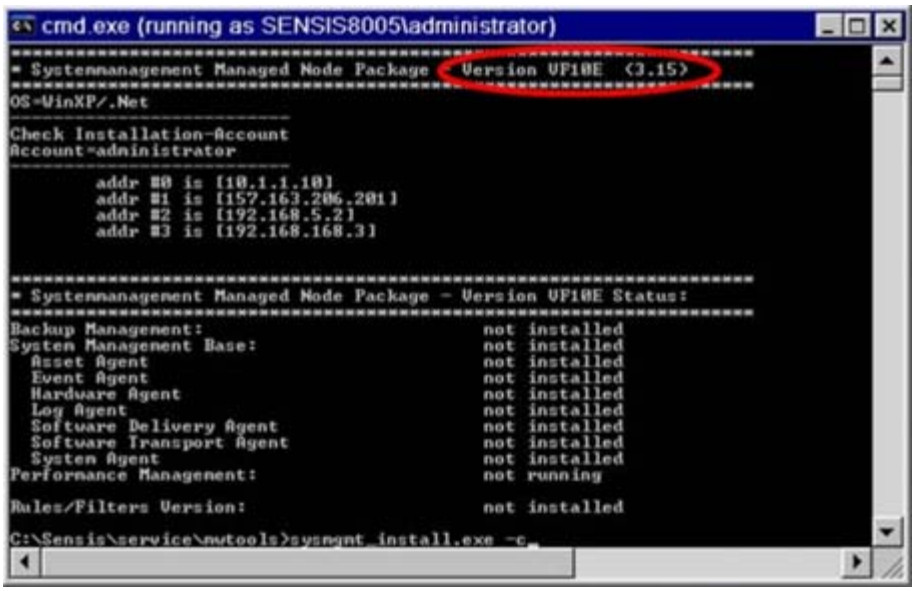
cmd.exe (running as SENSIS8005\administrator)
= Systemmanagement Managed Node Package - Version VP10E (3.15)
OS=WinXP/.Net
Check Installation-Account
Account=administrator
addr #0 is [10.1.1.10]
addr #1 is [157.163.206.201]
addr #2 is [192.168.5.2]
addr #3 is [192.168.168.3]
= Systemmanagement Managed Node Package - Version VP10E Status:
Backup Management: not installed
System Management Base: not installed
Asset Agent not installed
Event Agent not installed
Hardware Agent not installed
Log Agent not installed
Software Delivery Agent not installed
Software Transport Agent not installed
System Agent not installed
Performance Management: not running
Rules/Filters Version: not installed
C:\Sensis\service\mwtools>sysmgmt_install.exe -c_

Fig. 9: MNP version check

Procedure

- Start the Service SW.

- Open a DOS windows (command prompt).
- Enter the command **<tracert "IP address">**.

  The syntax of the command depends on the time zone in which the system is located and which MNP version (VExx / VFxx or VGxx) is used.

Tab. 1 Tracert commands for MNP versions VExx and VFxx

Time Zone	Enter the command under Parameters	Explanation of the Command
I (Europe, Africa)	tracert 194.138.39.18	traces route to the RDiag server, Fürth
	tracert 194.138.39.20	traces route to the Event Mgmt. and Asset Mgmt. server, Fürth
	tracert 194.138.39.22	traces route to the SW Distribution server, Fürth
II (America)	tracert 129.73.116.92	traces route to the RDiag server, Newark
	tracert 129.73.116.90	traces route to the Event Mgmt. and Asset Mgmt. server, Newark
	tracert 129.73.116.94	traces route to the SW Distribution server, Newark
III (Asia, Australia)	tracert 194.138.243.178	traces route to the RDiag, Singapore
	tracert 194.138.243.180	traces route to the Event Mgmt. and Asset Mgmt. server, Singapore
	tracert 194.138.243.182	traces route to the SW-Distribution server Singapur / Newark

Tab. 2 Tracert commands for MNP version VGxx

Time Zone	Enter the command under Parameters	Explanation of the Command
I (Europe, Africa)	tracert 194.138.39.18	traces route to the RDiag server, Fürth
	tracert 194.138.39.19	traces route to the Event Mgmt. and Asset Mgmt. server, Fürth
	tracert 194.138.39.21	traces route to the SW Distribution server, Fürth

Time Zone	Enter the command under Parameters	Explanation of the Command
II (America)	tracert 129.73.116.92	traces route to the RDiag server, Newark
	tracert 129.73.116.91	traces route to the Event Mgmt. and Asset Mgmt. server, Newark
	tracert 129.73.116.93	traces route to the SW Distribution server, Newark
III (Asia, Australia)	tracert 194.138.243.178	traces route to the RDiag, Singapore
	tracert 194.138.243.179	traces route to the Event Mgmt. and Asset Mgmt. server, Singapore
	tracert 194.138.243.181	traces route to the SW-Distribution server Singapur / Newark

NOTE

As described on the following pages, the IP addresses 157.163.201.XXX should be viewed only as examples and are not obligatory!

Example:

Tracing to the SRS server in Fürth, time zone I.

With the tracert 194.138.39.18 command, a connection test to the SRS server in Fürth is performed. All gateways located between the medical system and the SRS router in Fürth are listed.

In this example, this is the Default/Local Gateway 157.163.201.61.

The SRS router has the IP 157.163.201.59

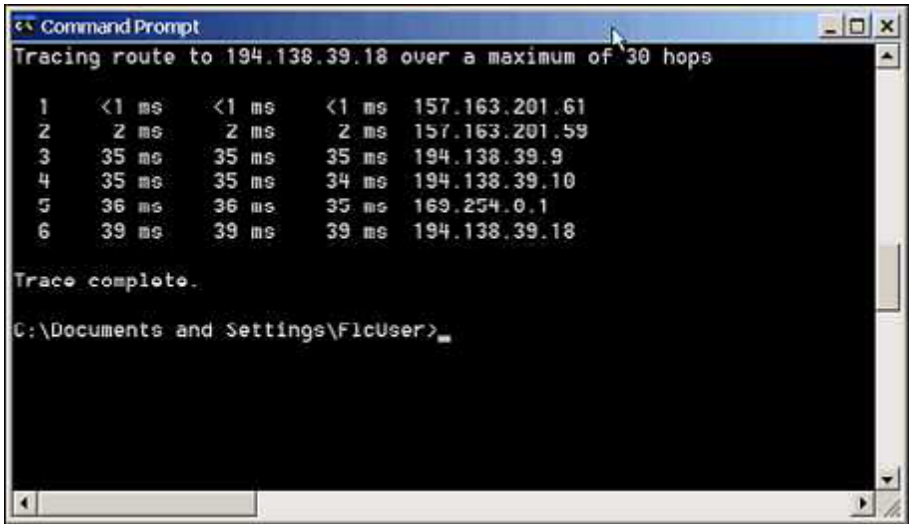
Command Prompt
Tracing route to 194.138.39.18 over a maximum of 30 hops
1 <1 ms <1 ms <1 ms 157.163.201.61
2 2 ms 2 ms 2 ms 157.163.201.59
3 35 ms 35 ms 35 ms 194.138.39.9
4 35 ms 35 ms 34 ms 194.138.39.10
5 36 ms 36 ms 35 ms 169.254.0.1
6 39 ms 39 ms 39 ms 194.138.39.18
Trace complete.
C:\Documents and Settings\FlcUser>

Fig. 10: Connectivity test successful

NOTE

A telephone connection requires some time to be established. For this reason it is possible that the “tracert” program will reach a time limit ((“time out”) and the message “Destination host is unreachable" or "request timeout" will be displayed. In this case, enter the "tracert” command again after approx. 30 s to test the function again.

Example for a “timeout”** of the “**tracert”** command:**

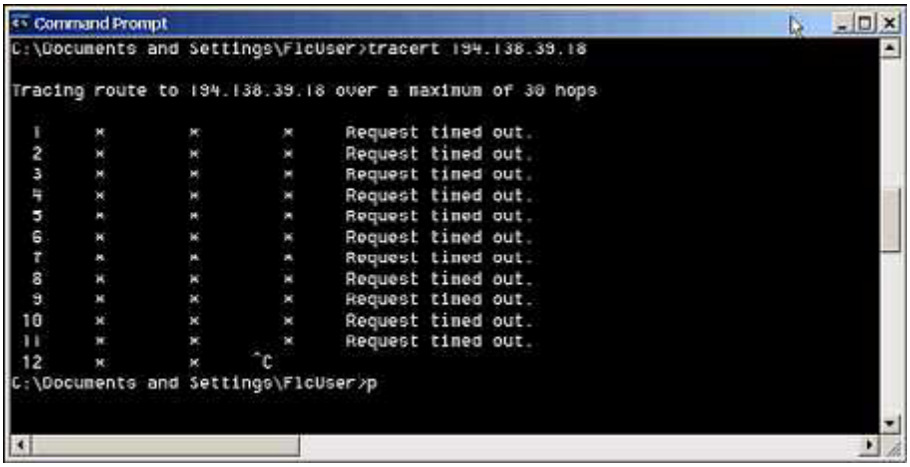
Command Prompt
C:\Documents and Settings\FlcUser>tracert 194.138.39.18
Tracing route to 194.138.39.18 over a maximum of 30 hops
1 * * * Request timed out.
2 * * * Request timed out.
3 * * * Request timed out.
4 * * * Request timed out.
5 * * * Request timed out.
6 * * * Request timed out.
7 * * * Request timed out.
8 * * * Request timed out.
9 * * * Request timed out.
10 * * * Request timed out.
11 * * * Request timed out.
12 * * ^C
C:\Documents and Settings\FlcUser>p

Fig. 11: Connectivity test failed

If the desired server (Fürth, Newark or Singapore) still cannot be reached, even after several attempts, the SRS Help Desk and/or the hospital's network administrator must be contacted for troubleshooting.

Example: IP connection to the SRS server does not work

Here, the medical system is connected via the local gateway 157.163.201.61 and via the SRS router 157.163.201.59 (medical system / Default/Local Gateway and the router are in the same network) to the SRS server in Fürth/Germany, IP 194.138.39.18.

NOTE

In some network configurations it is possible that the “Internet Control Message Protocol” will be blocked. In such cases, the “Ping” does not work. In this case, perform a connection test (Test Ping not Alive / p. 29) with the telnet command on the corresponding server. If this test also fails, the SRS Help Desk (Help Desk / p. 76) has to be contacted immediately.

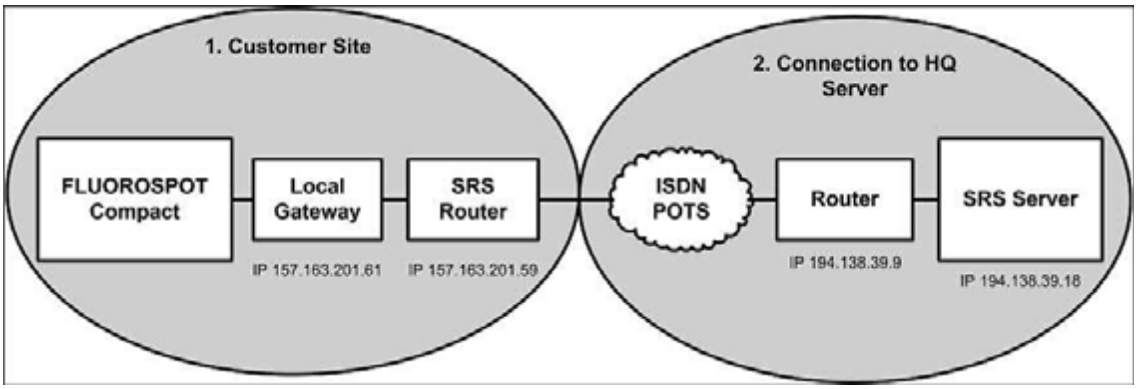

Fig. 12: Troubleshooting the Router - Example of Network Environment

Possible Error Message #1

The medical system cannot reach the SRS router **at the customer's on-site location.**

The problem is displayed in the "tracert" window as follows:

Tracing route to 194.138.39.18 over a maximum of 30 hops.

hop #	Time 1	Time 2	Time 3	Message
1	*	*	*	Request timed out
2	*	*	*	Request timed out
n[1]	*	*	*	Request timed out
				Desination host unreachable[2]

1. n: The maximum is 30 hops
2. If the trace encountered no errors, the following message is displayed: Trace complete.

Error Cause	Troubleshooting
The Gateway is not properly defined in the medical system.	Check the configuration of the Gateways and possible static Route and correct it.

Error Cause	Troubleshooting
The SRS/customer router is not properly installed or configured.	Check the installation and configuration of the SRS router. The router must be switched on and started and the Ethernet cable must be plugged in. On Cisco routers, the green LED LNK next to the Ethernet connector shows that the Ethernet cable has been connected properly. If this LED is **OFF**, it is possible that the wrong cable (cross cable / straight cable) is used. Some routers have a button to cross the input signal. In this case, press the button and check whether the green LNK LED is now **ON**.
The Hospital Routing is not correct in a situation in which the medical system and the router are not in the same network area.	The network administrator of the hospital must check the routing in the hospital. The SIEMENS representative must check the router configuration.

Possible Error Message #2

The medical system can reach the SRS router **on-site at the customer, but not the SRS router at headquarters.**

The problem is displayed in the "tracert" window as follows:

Tracing route to 194.138.39.18 over a maximum of 30 hops.

hop #	Time 1	Time 2	Time 3	Message
1	<10 ms	<10 ms	<10 ms	..... [157.163.201.59]
2	*	*	*	Request timed out
n[1]	*	*	*	Request timed out
				Desination host unreachable[2]

1. n: The maximum is 30 hops
2. If the trace encountered no errors, the following message is displayed: Trace complete.

Error Cause	Troubleshooting
The customer router is not properly configured.	Request support, either from the hospital's network administrator or the responsible department at the SRS Help Desk (Help Desk / p. 76), depending on who is responsible for the router configuration.
An incorrect telephone connection or the phone connection does not allow outgoing calls.	Request support, either from the hospital's network administrator or the responsible department at the SRS Help Desk (Help Desk / p. 76), depending on who is responsible for the router configuration. Connect the router at the correct phone connection.
The SRS router at the headquarters is not configured properly.	Request support from the SRS Help Desk (Help Desk / p. 76).

Possible Error Message #3

The medical system can reach the SRS router **at headquarters, but not the SRS server.**

The problem is displayed in the "tracert" window as follows:

Tracing route to 194.138.39.18 over a maximum of 30 hops.

hop #	Time 1	Time 2	Time 3	Message
1	<10 ms	<10 ms	<10 ms	..... [157.163.201.61]
2	<10 ms	<10 ms	<10 ms	..... [157.163.201.59]
3	<200 ms	<200 ms	<200 ms	..... [194.138.39.9]
n[1]	*	*	*	Request timed out
				Desination host unreachable[2]

1. n: The maximum is 30 hops
2. If the trace encountered no errors, the following message is displayed: Trace complete.

Error Cause	Troubleshooting
The server cannot be accessed.	After an appropriate delay time, try again to access the server. If the server still cannot be accessed, inform the SRS Help Desk (Help Desk / p. 76).

Test Ping not Alive

NOTE

In some network configurations it is possible that the "Internet Control Message Protocol" will be blocked. In such cases, the "Ping" does not work. In this case, perform a connection test (Test Ping not Alive / p. 29) with the telnet command on the corresponding server. If this test also fails, the SRS Help Desk (Help Desk / p. 76) has to be contacted immediately.

1. Select **Utilities** on the Service Home page.
2. Select **Escape to OS**.
3. Enter den text **start cmd** ↵ in the "Parameters" box. Then click on **Go** in the "Action Bar". A Command opens.
4. Depending on the Remote Service Center and the installed MNP version (VExx / VFxx or VGxx), enter the particular Telnet command for the SRS server and System Management server in the "**Command**" window, e.g. **telnet 194.138.39.18 21**.

Tab. 3 Telnet Commands for SRS Environment based on MNP versions VExx and VFxx

Remote Server Center	SRS server	System Management Server
Europe / Africa	telnet 194.138.39.18 21	telnet 194.138.39.22 1721 (FTHW9MVA)
USA / America	telnet 129.73.116.92 21	telnet 129.73.116.94 1721 (SRSSQL03)
Asia, Pacific	telnet 194.138.243.178 21[1]	telnet 194.138.243.182 1721 (SGPT3182A)

1. telnet, IP address, User Port 21

Tab. 4 Telnet Commands for SRS Environment based on MNP version VGxx

Remote Server Center	SRS server	System Management Server
Europe / Africa	telnet 194.138.39.18 21	telnet 194.138.39.21 12061 (FTHW9MUA)
USA / America	telnet 129.73.116.92 21	telnet 129.73.116.93 12061 (SRSSQL02)
Asia, Pacific	telnet 194.138.243.178 21[1]	telnet 194.138.243.181 12061 (SGPT3181A)

1. telnet, IP address, User Port 21

5. With a successful connection, the **System Mangement Server** logs on with its **Host name** and the **SRS server** with its **FTP account** and the **IP address**.

   To leave the Telnet connection, enter the key combination **CTRL**, **+** and ↵. Then terminate the connection with **Quit**.

6. A bad connection with the message: **Connecting to 194.138.39.18 ... Could not open to host port 21: Connection failed** is sent out. In this case, immediately contact the SRS Help Desk (Help Desk / p. 76) for error analysis.

Handling the Pre-Connect Tool

The following chapters describe the handling of the SRS Pre-Connect Tool if there are installation or configuration problems.

NOTE	**It is strictly forbidden to install the Pre-Connect Tool on medical systems.**

Checking all Prerequisites

Before using the Siemens Pre-Connect Tool (PCT), check the following prerequisites:

- Check to make sure all the required system network information is on hand:
  - System IP address
  - If Inside NAT is being used, make note of the system's Inside NAT IP address.

    If you are not sure, ask the hospital network administrator or ask the SRS Help Desk; see "Additional Information".
  - Subnet mask
  - Gateway IP address
- The PCT must be installed on the CSE's service laptop.

  The PCT is available in the Intranet; see "Additional Information".

NOTE	**With every start of the PCT, the tool checks whether:** **- a new version of PCT is available** **- a new version of product model database is available** **With one of these cases, the PCT automatically triggers a restart.** **Please confirm the restart messages to load the correct settings.** **If you have any questions, please ask the SRS Help Desk; see "Additional Information".**

Test Procedure

1. Disconnect the network cable from the system.

NOTE

If there are two network cables, first find out which is the correct cable; it will be the one connected to the "DICOM" TCP/IP stack.

From the information given for the TCP/IP stack, you can find out what physical connections are present:

--> Perform the command "ipconfig /all", and in the output look for the value "Description".

2. Connect this cable to your service laptop.

3. Boot your laptop and start the PCT.

   The SRS date base, which includes the TCP/IP network ports of the system (MNP agent software), will be loaded into the laptop.

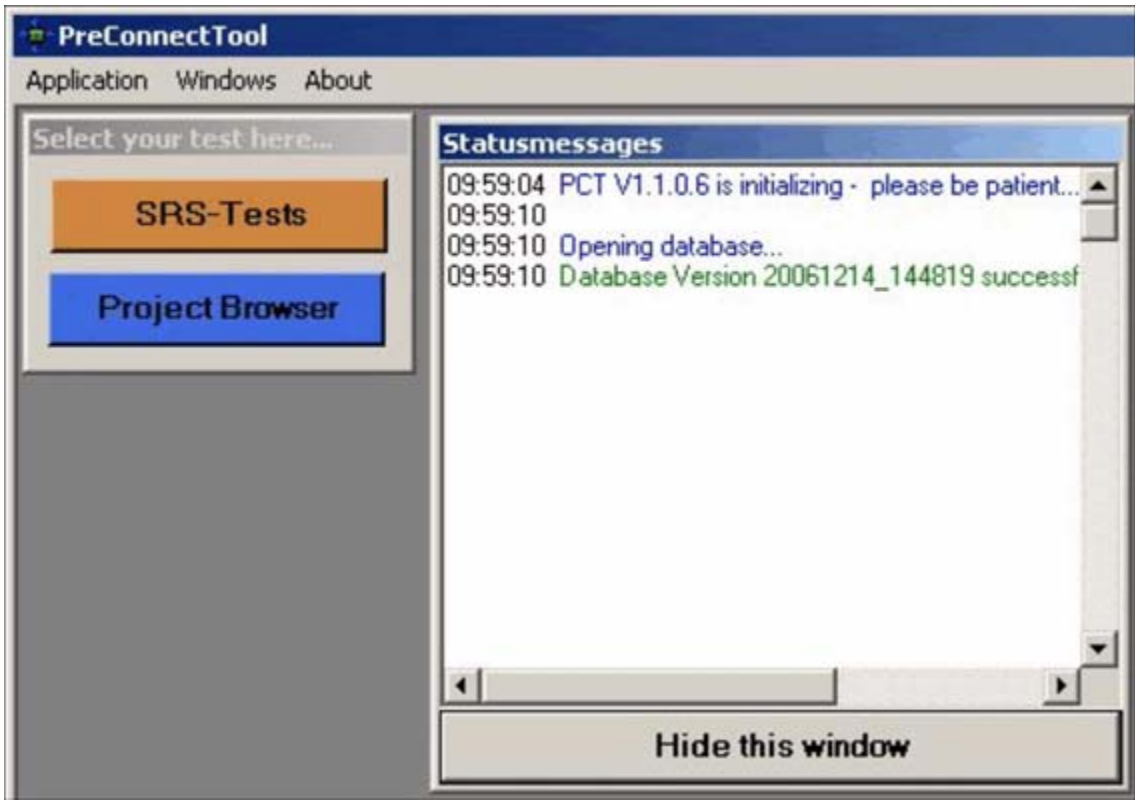

Fig. 13: Start page of Pre-Connect Tool

Continue by clicking on “Application” --> “Network Device”

4. Activate the network card by selecting the checkbox as shown in the illustration (item 1).

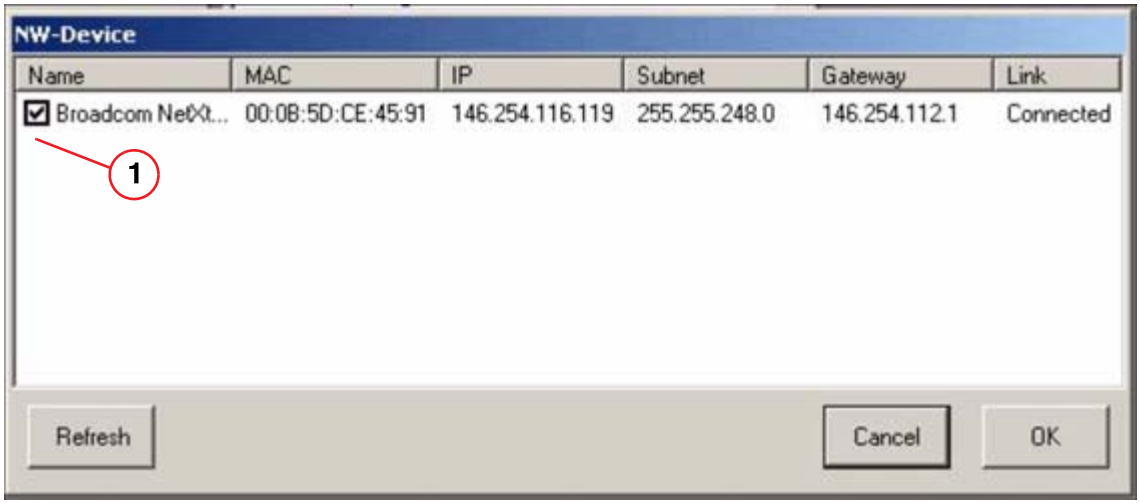

Fig. 14: Select the network card for the Pre-Connect test

Pos. 1 Checkbox to select

5. Create the “Customer Site” (site name and customer country) and click on “Create”; see illustration.

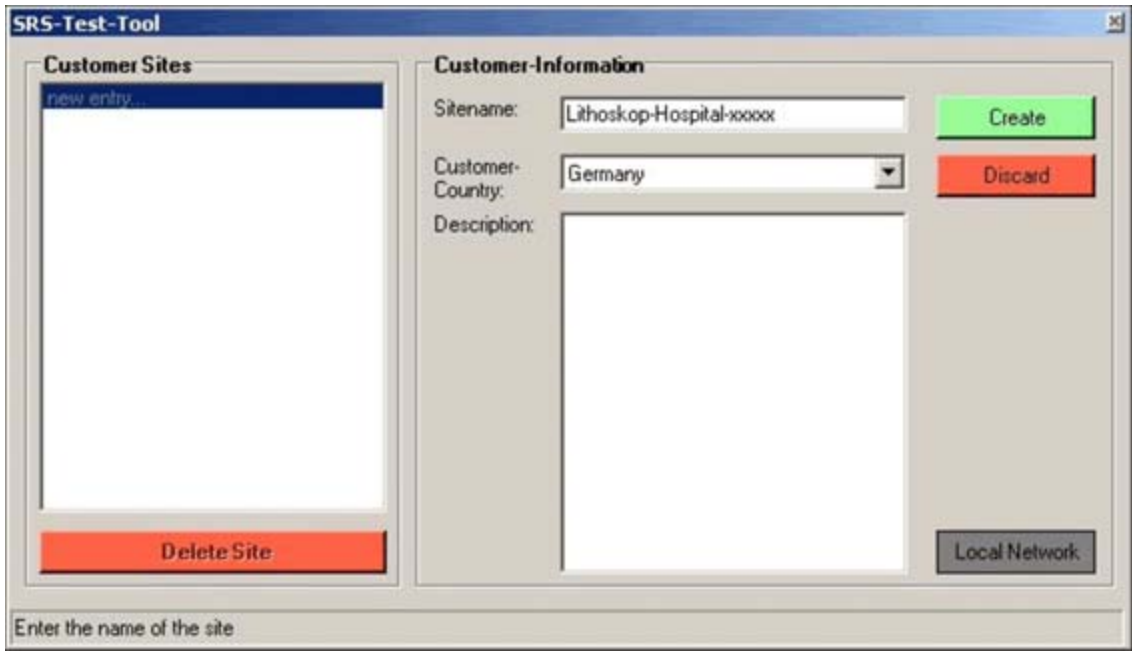

Fig. 15: Create customer site

6. After creating, click on “Local Network”; see item 1

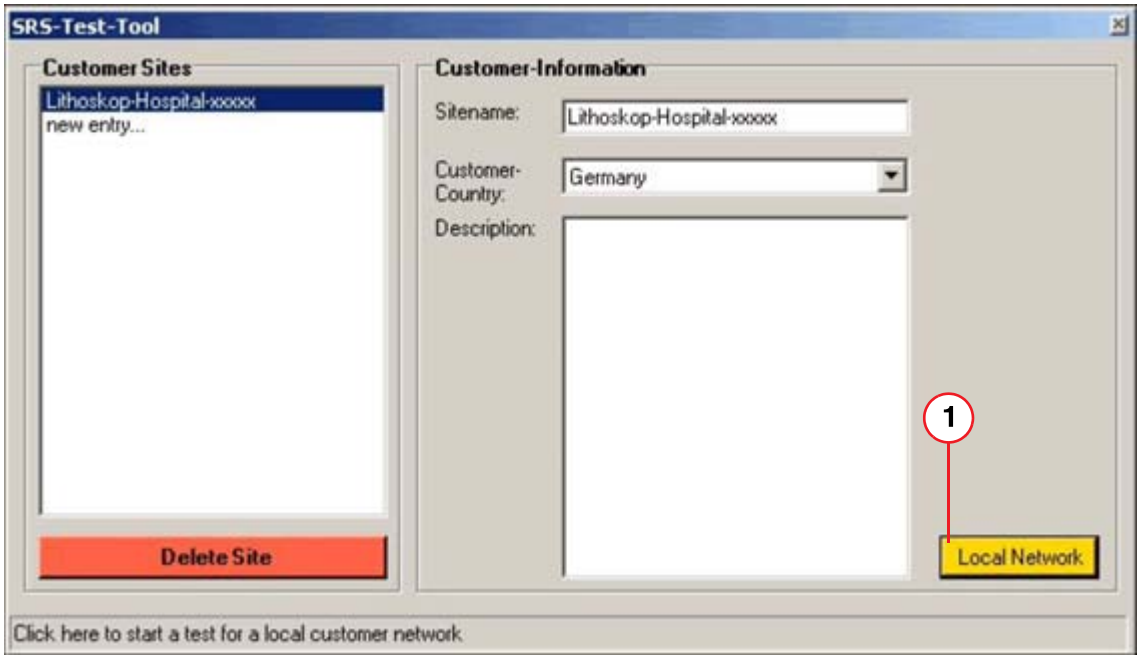

Fig. 16: Set “Local Network”

Pos. 1 Click on the “Local Network” button

7. Fill in the form with the required information; see illustration:
   - network-specific (IP address, subnet mask, NAT IP address if using Inside NAT, customer’s SRS gateway) see item 1.

     If you have any questions at this point, please ask the SRS Help Desk; see "Additional Information".
   - system-specific (modality, product and model) see item 2

Click on “Save” (see item 3) to complete customizing

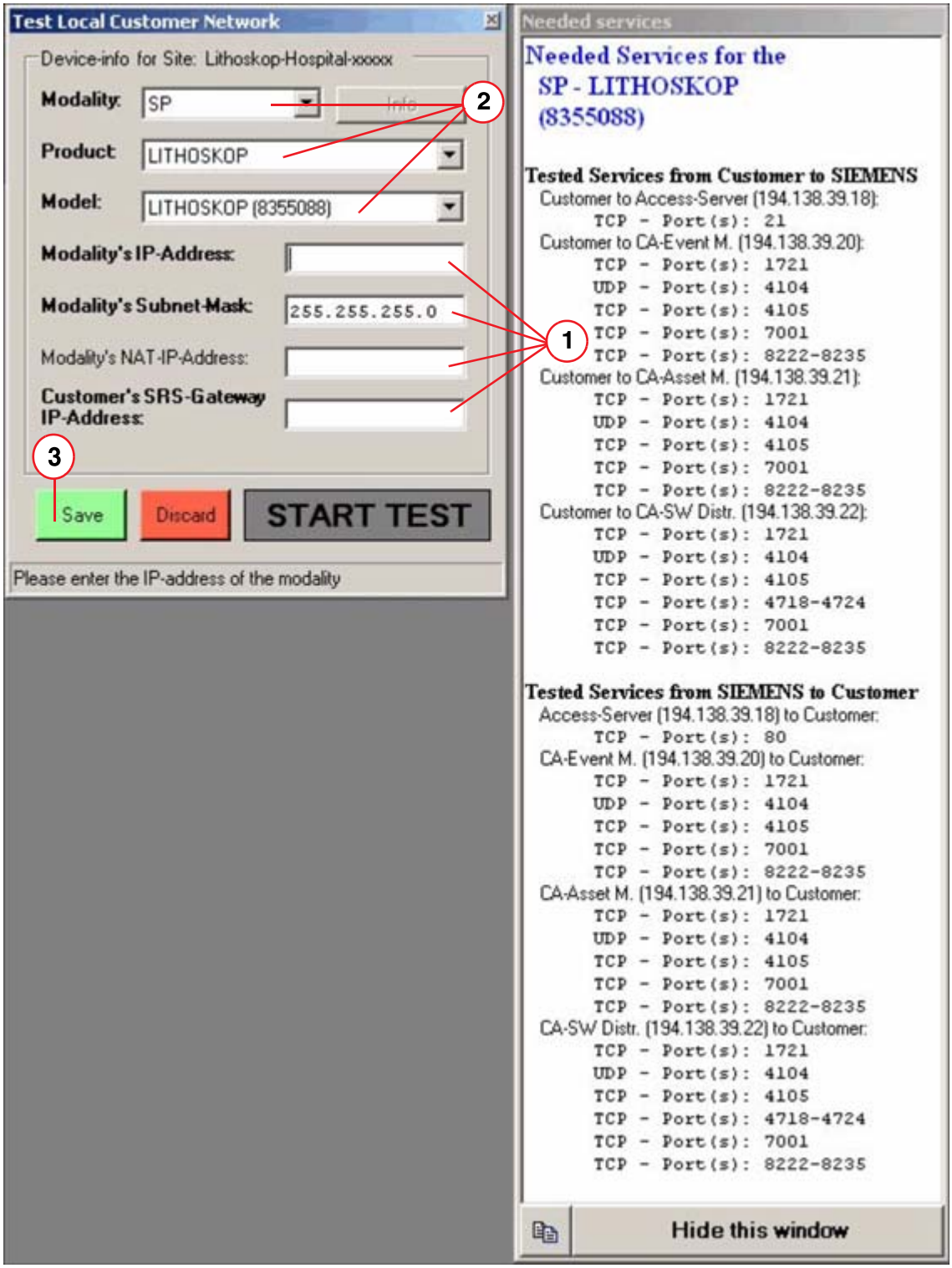

Fig. 17: Values for the test

Pos. 1 Network values

Pos. 2 System values

Pos. 3 “Save” button to save all values

8. After “Save” is pressed, the following page is displayed:

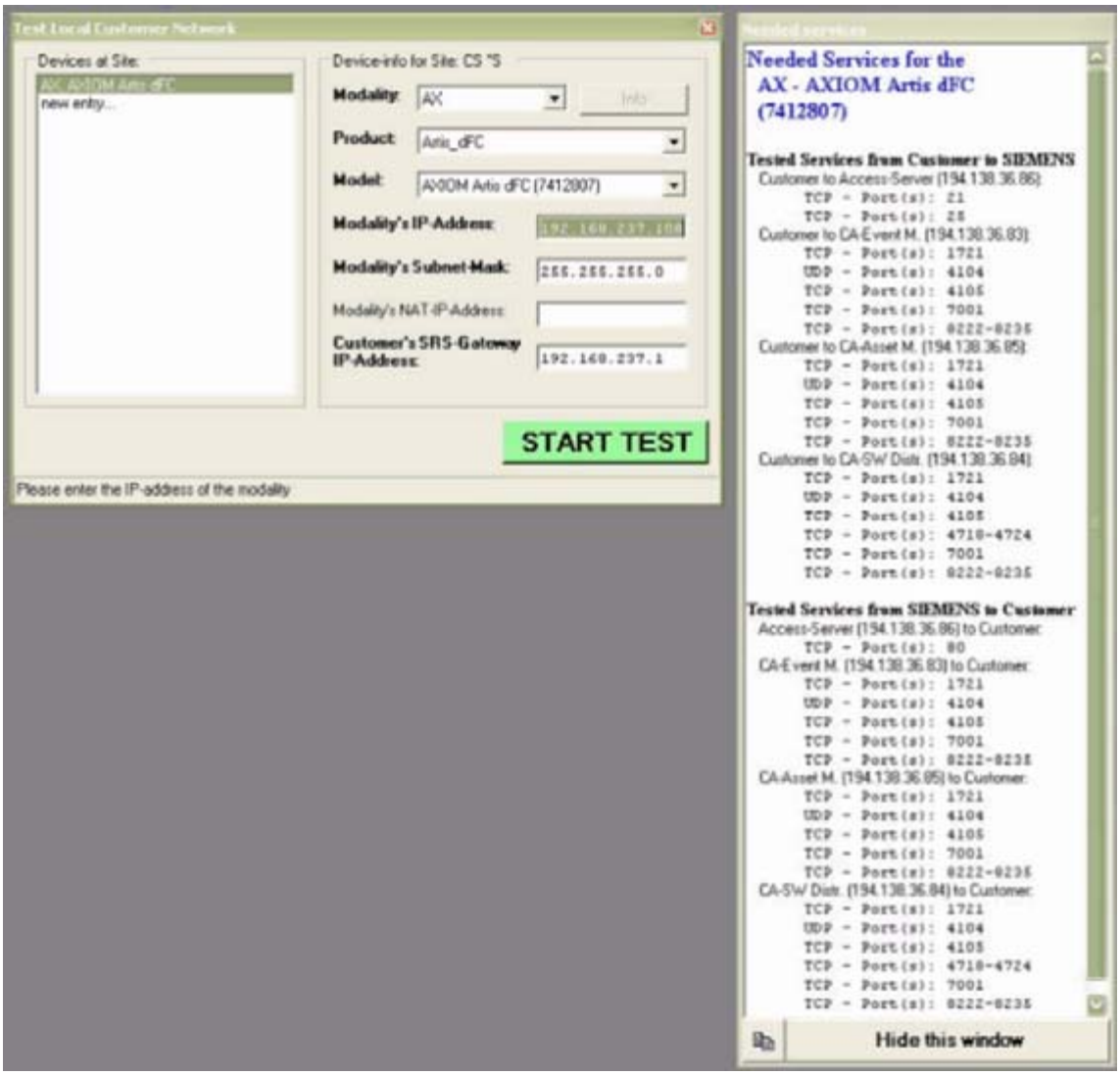

Fig. 18: Pre-Connect Tool settings with user port list

Click on “START TEST” to start the test.

NOTE	**The test takes approximately 5 - 10 minutes!**

9. Completing the test

   If the test is successful, a green message (see item 1) is displayed.

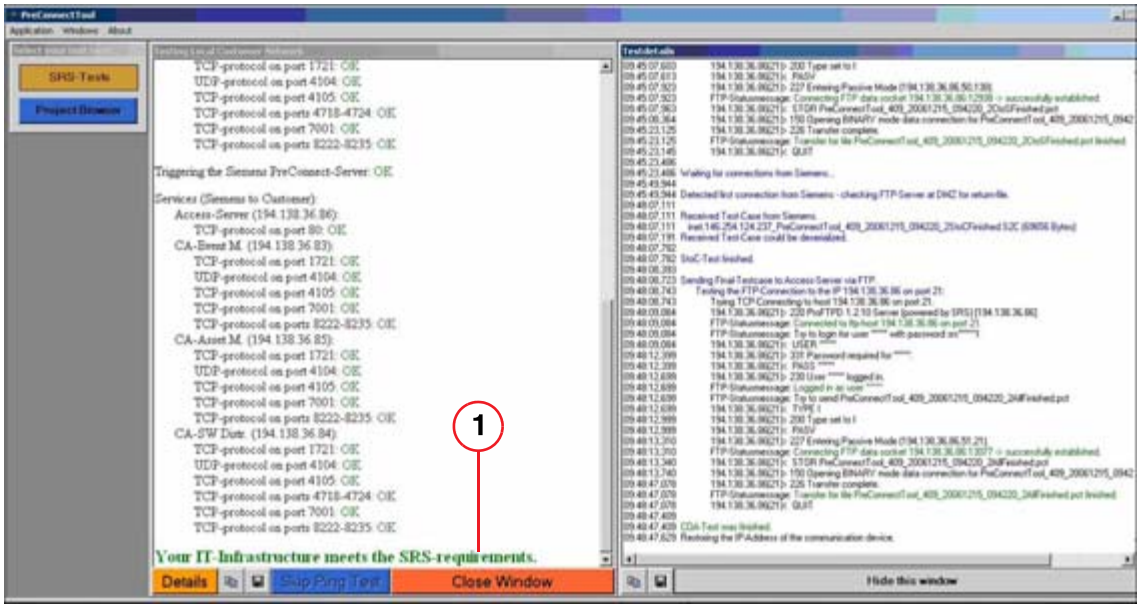

Fig. 19: Example of a successful test

Pos. 1 "Success" message with text in green

If the test is not successful, perform the following:

a) save the output files to your laptop.

b) show the output files to the hospital's network administrator to have the network settings of the the hospital network environment corrected.

c) or send the files to the SRS Help Desk (see "Additional Information") to have the network settings in the SRS environment corrected.

Following the corrective actions, run the SRS test again.

10. Complete the test by performing the following steps:

    a) After the test has been performed with a successful outcome, complete the test program as follows:

       click on “Application” --> “Exit”

    b) Disconnect the network cable from the laptop

    c) Connect the network cable to the system (in the same location as before).

Reactive Remote Service via CORINA

Problems with Remote Service via CORINA

Due to the security policy, only known network bands are allowed to route over the “Inner Fire Wall” to customer systems.

If the connection to the customer system that is in operation fails with the error message `“... a firewall might be blocking the ping request...”`.

At the remote portal

- Login to the remote portal
- Select the link for the `test connection to access Server`.

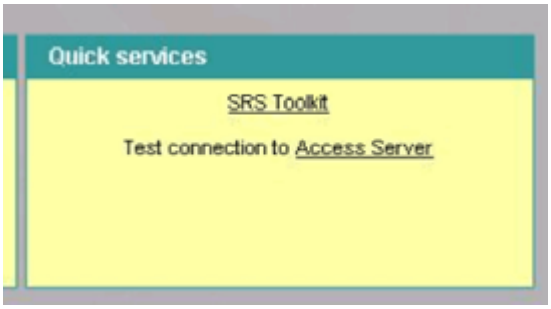

Fig. 20: Testing the Connection Link

- Accept the certificate download and install the certificate

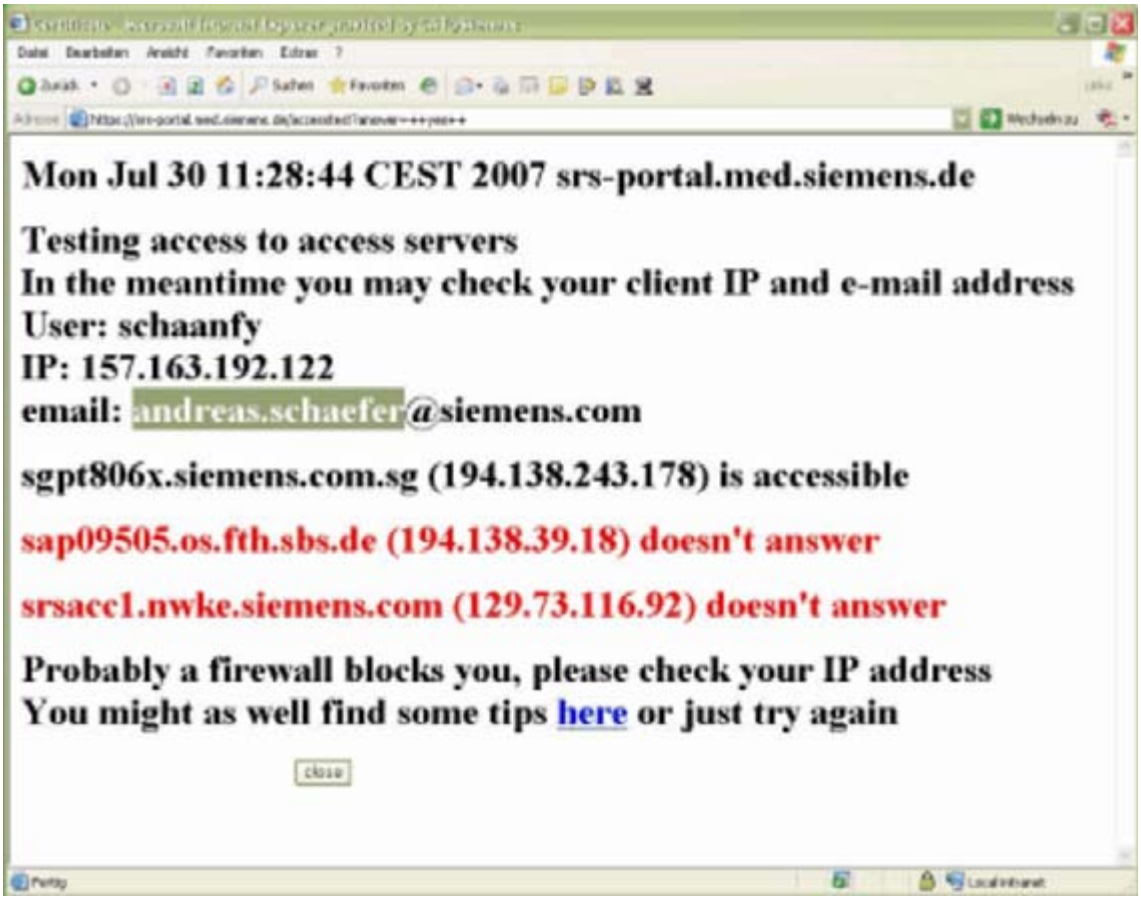
Mon Jul 30 11:28:44 CEST 2007 srs-portal.med.siemens.de
Testing access to access servers
In the meantime you may check your client IP and e-mail address
User: schaanfy
IP: 157.163.192.122
email: andreas.schaefer@siemens.com
sgpt806x.siemens.com.sg (194.138.243.178) is accessible
sap09505.os.fth.sbs.de (194.138.39.18) doesn't answer
srsacc1.nwke.siemens.com (129.73.116.92) doesn't answer
Probably a firewall blocks you, please check your IP address
You might as well find some tips here or just try again
close

Fig. 21: Failed Access Server test

At your local PC

- Simultaneously press the **Windows key** and **R**
- Enter the command **cmd** and click on **OK**.
- In the cmd window, enter the command **ipconfig -all**

Please contact the `SRS Help Desk` (Help Desk / p. 76) to check /add your CORINA network to the SRS “Inner Fire Wall” list

Basic Ports

From the Customer System (Modality) to Siemens (DMZ)

Protocol	Destination Port	Description
TCP	20, 21	FTP
TCP	25	SMTP
TCP	80	HTTP
TCP	443	HTTPS
TCP	8080	HTTP for Knowledge Base and Life net
TCP	8085	HTTP

From Siemens (DMZ) to the Customer System (Modality)

Protocol	Destination Port	Description
TCP	20, 21	FTP
TCP	80	HTTP
TCP	443	HTTPS
TCP	8080	HTTP for Knowledge Base and Life net
TCP	8085	HTTP

FTP

To allow usage of pre-configured auto reports, the logical name for the FTP target must be configured regarding installation information provided for the business unit (e.g. AX, CT, MR, SP, etc....).

RDIAG Server (FTP Target Server)

Three worldwide access servers make your system accessible to Siemens Remote Service.

Time zone / Server function	**I (Europe, Africa) Fuerth**	**II (America) Newark**	**III (Asia, Australia) Singapore**
SRS Access Server[1] **See note**	LUX09505 **194.138.39.18**	SRSACC1 **129.73.116.92**	SGPT806X **194.138.243.178**

1. This is the target server for the configuration of the FTP transfer functionality in the modality service configuration

NOTE

If the customer uses a network configuration with Outside NAT (Outside NAT / p. 20), another IP address for the RDIAG (SRS access) server is needed and is assigned by the hospital network administrator.

Password

The only password needed during the SRS configuration is the connection password for access via FTP to the SRS access server (account “rdiagftp”).

The password is listed in the CS Knowledge Base see (Passwords / p. 88).

FTP Test Transfer

Test the `FTP connection` to the RDIAG server (Syngo-based systems):

- Open Local Service
- Select `File&Image Tools`

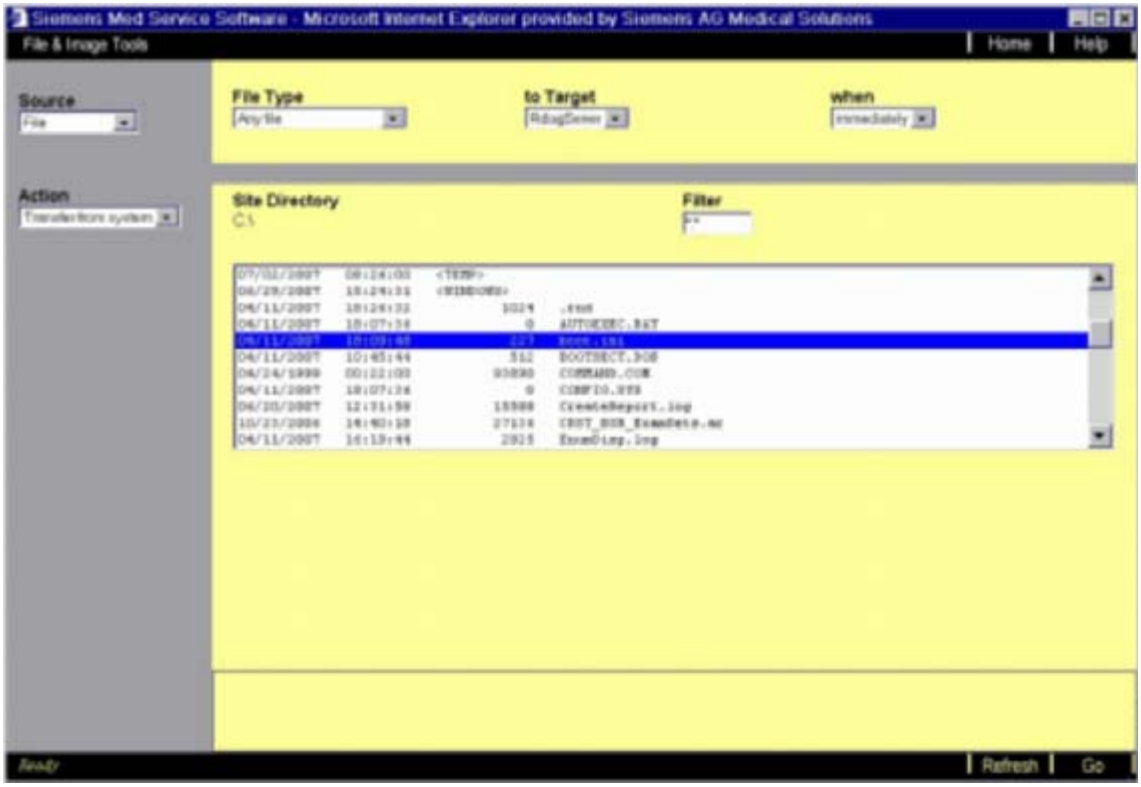

Fig. 22: File & Image Tool

- Select `Source`: **<File>**
- Select `Action`: **<Transfer from System>**
- Select `File Type`: **<Any file>**
- Select `to Target`: **<DRiagServer>**
- In `Site directory c:\`, select the **boot.ini** line in the window.
- Start the file transfer with **GO** in the Action bar.

  The `Files & Image transfer Progress Info` window opens.

  The transfer is successfully concluded when **100%** is behind done and **transfer successfully finished** appears behind `transfer status`.

  ➪ If the connection is not okay, the reason for this must be found and corrected (e.g. incorrectly configured router). For troubleshooting, the SRS Help Desk must be contacted (Help Desk / p. 76).

- Press **Close Window** to close the `File & Image Transfer Progress Info`

Syngo Auto Transfer List

If the customer agrees, automatic transfer of auto reporting messages or System Management Event messages may be enabled here. Deactivate this option only if the customer does not allow automatic data transfer.

Deleting the Transfer List

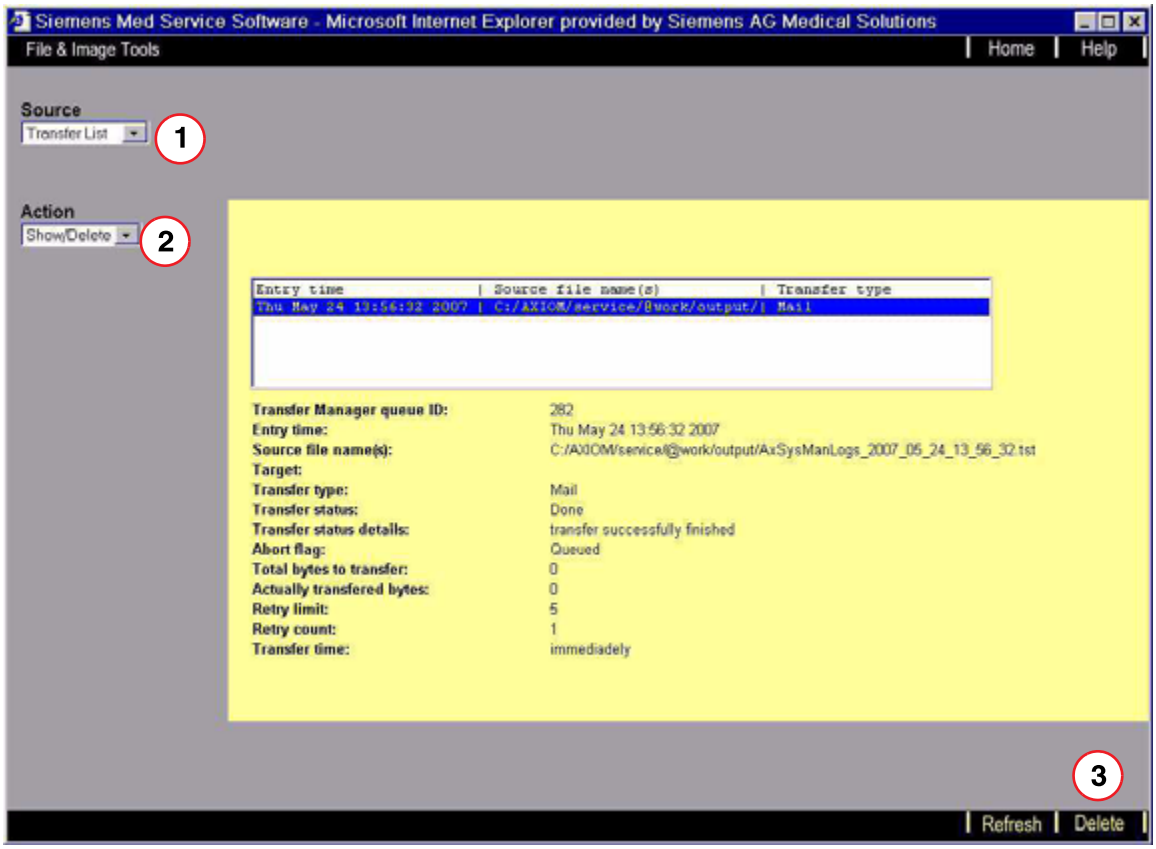

Fig. 23: File & Image Tools Transfer List

Pos. 1 Transferlist

Pos. 2 Show/Delte

Pos. 3 Delete

- Open Syngo Service
- Select `File & Image Tools`
- Select **Transfer List** under `Source` (1/Fig. 23 / p. 43)
- Select **Show/Delete** under `Action` (2/Fig. 23 / p. 43)
- Select the unused jobs step by step and press **Delete** (3/Fig. 23 / p. 43)

  `Deletion can take up to 5 minutes.`

  Some jobs cannot be deleted, please refer to the next chapter.

File & Image Transfer does not work

`File & Image transfer` does not work, no contents are displayed under **C:**.

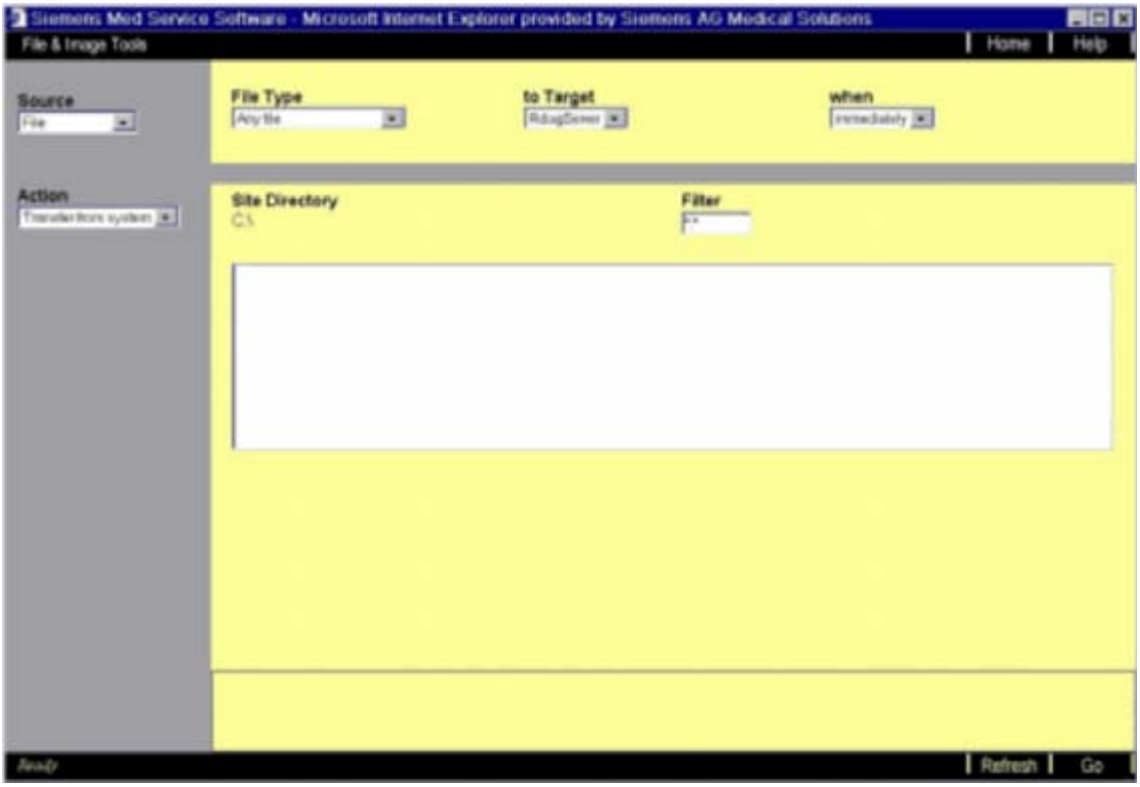

Fig. 24: Transfer list does not work

- Gain access to the system via SRS with **Full Access**, or do it locally at the system.

- **Stop Auto Report** by deselecting all Auto Report templates.
  - Open Syngo Service **Auto Report**
  - Check which templates are active (1/Fig. 25 / p. 45)
  - `Deactivate` the template and **Save** the status (2/Fig. 25 / p. 45)

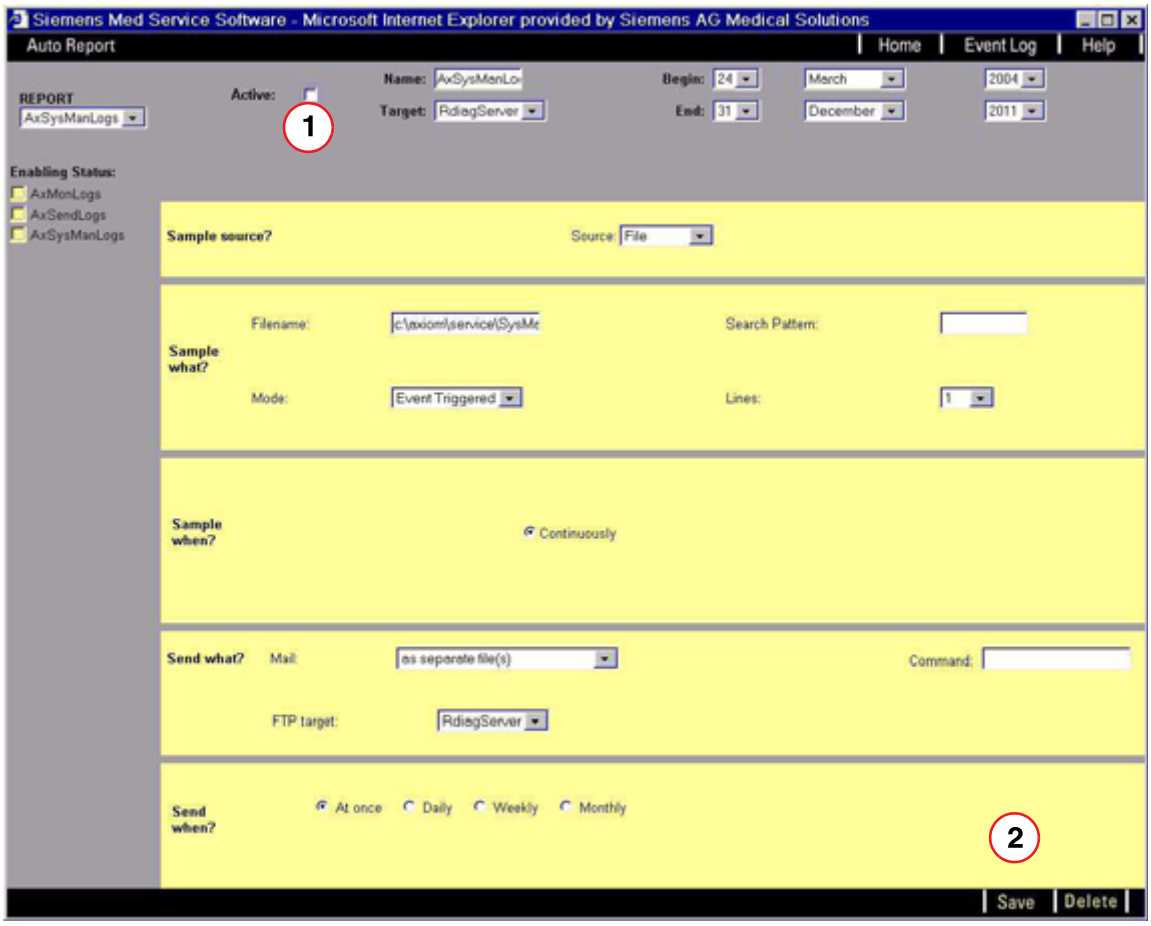

Fig. 25: Auto Report

Pos. 1 Deactivate

Pos. 2 Save

- **Close** Syngo Service and **reboot** the system.
- Clear the job queue
  - Open a command shell
  - Enter: **sc stop transfermgr** ↵
  - Enter: **sc query transfermgr** ↵ (transfer manager should be stopped)
  - Enter: **delete C:\AXIOM\config\service\transfermgr.tmc** ↵ (delete the job file)

NOTE	**"AXIOM" is an example for the %medhome% system path, please accept the patch that is used in your system.**

  - Enter: **sc start transfermgr** ↵
  - Enter: **sc query Transfermgr** ↵ (transfer manager should be started)

The job queue should be empty now:

Activate the `Auto Report Template` again which had been deactivated previously.

Reboot the system to make sure that everything is up and running again.

How to find out %Medhome%

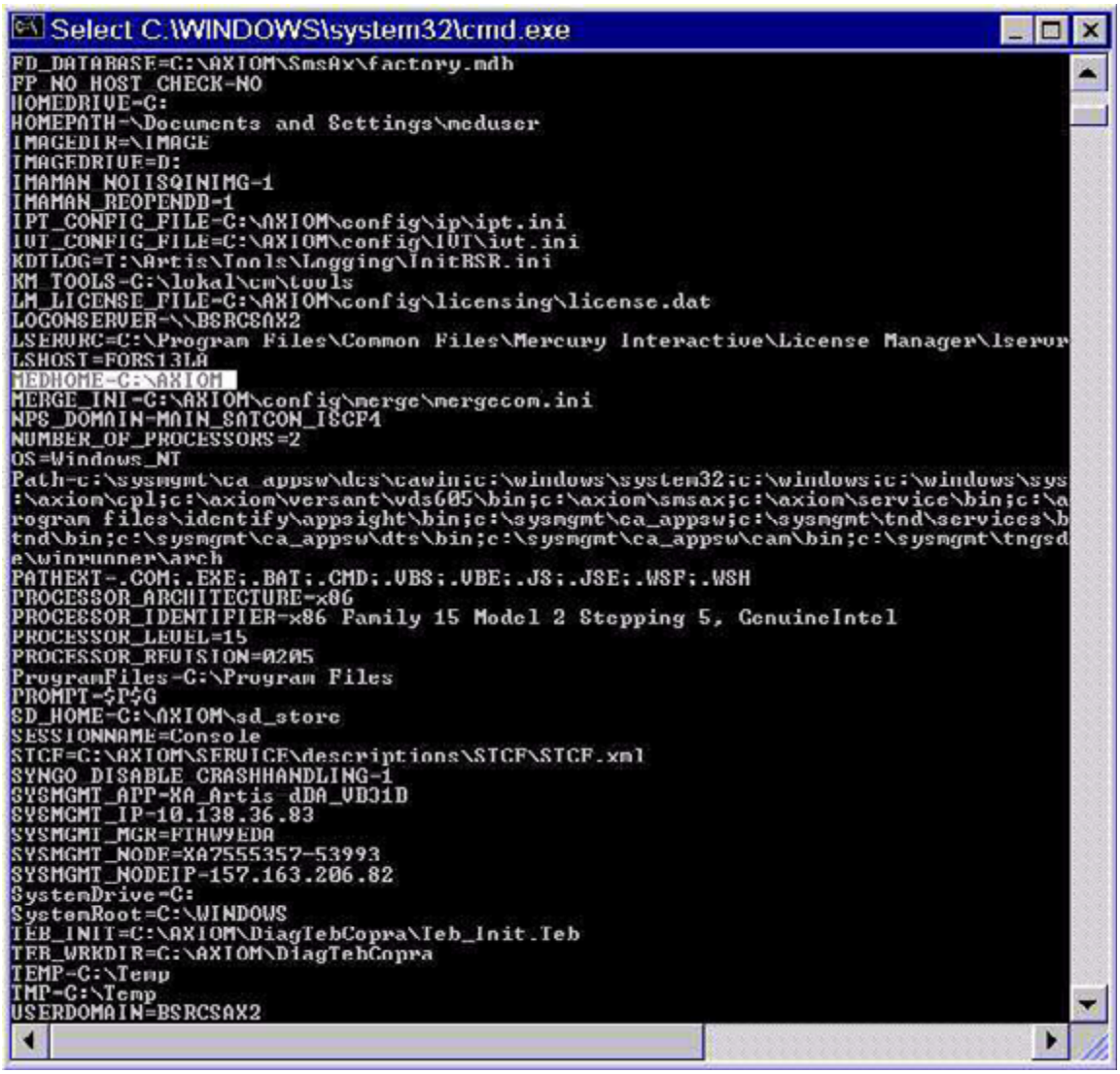

Fig. 26: MEDHOME Variable

- Open a Command shell
- Enter: **set** ↵
- Search for the string that begins with **MEDHOME**

Mail

Check the host name and IP address of the mail targets. (RAS is not supported by syngo systems)

For more details, please refer to the System Configuration Instructions for Siemens Remote Service.

RDIAG Server

Three worldwide access servers make your system accessible to Siemens Remote Service.

Time zone / Server function	**I (Europe, Africa) Fuerth**	**II (America) Newark**	**III (Asia, Australia) Singapore**
SRS Access Server[1] **See note**	LUX09505 **194.138.39.18**	SRSACC1 **129.73.116.92**	SGPT806X **194.138.243.178**

1. This is the target server for the configuration of the mail transfer functionality in the modality service configuration

NOTE

If the customer uses a network configuration with Outside NAT (Outside NAT / p. 20), another IP address of RDIAG (SRS access) server is needed and is assigned by the hospital network administrator.

Mail Test

Sending an e-mail must function before Auto Report is activated!

The checkmark (1/Fig. 27 / p. 48) is set here only temporarily to test the e-mail connection. (Depending on the specifications of the Business Unit)

After successfully completing the test, the checkmark must be removed again. (Depending on the specifications of the Business Unit)

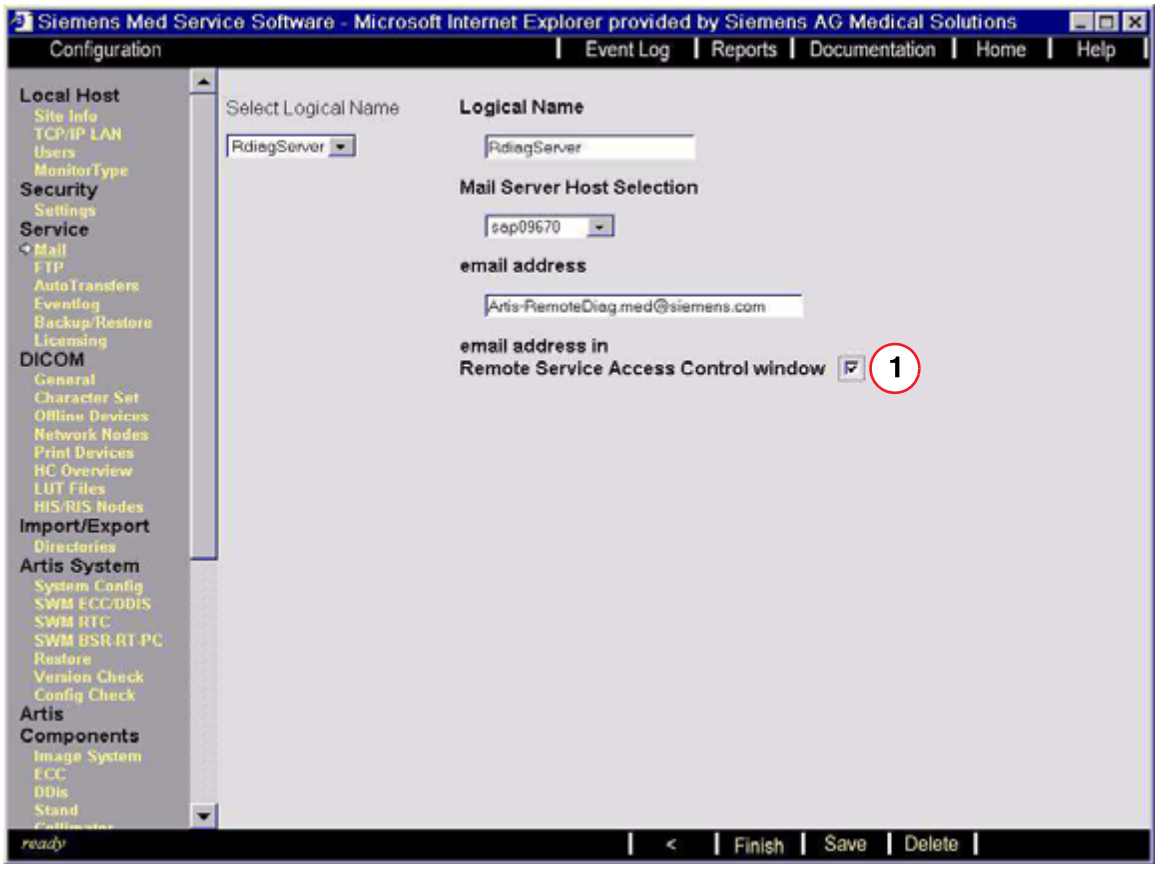

Fig. 27: Mail configuration

Pos. 1 Remote Service Access

- **Set a checkmark** (1/Fig. 27 / p. 48) for the "`e-mail address in the Remote Service Access Control window`" checkbox, save the change.
- Shut down the system and reboot it.
- On the text monitor, **move the cursor to the top edge of the screen**. In the selection bar that appears, first select **<Options>** **<Service>** and then **<Remote Service>**.
- Select the **<Mail>** item in the "Remote Service Access Control" window.
- The previously programmed mail target, e.g. "Artis-RemoteDiag.med@siemens.com", must be displayed in the "`Mail to Service`" window.

NOTE

For the needed e-mail address, refer to the System Configuration Guide.

- Under "`Subject`", enter a message (text) and then click on **<Submit>**.
- Confirm the window with the message "`Mail transfer request accepted`" with **<Ok>**.

  The e-mail will now be sent.

  If the mail was successfully sent, there is no new message! If no error message is displayed after approx. 5 minutes, it can be assumed that the transfer was successful.

  If there is a bad connection, an error message is displayed in the Remote Service window: "`Mail error:.....Transfer failed`".

NOTE	**If the connection is not okay, the reason for this must be found and corrected (e.g. incorrectly configured router, no selection from the hospital telephone system, ...). Please contact the SRS Help Desk (Help Desk / p. 76) for trouble-shooting assistance.**

- If the **E-mail sent is ok**: Deselect the `"e-mail address in Remote Service Access Control window"` checkbox again, save the change and reboot the system.

MNP Installation/Activation of VExx and VFxx Versions

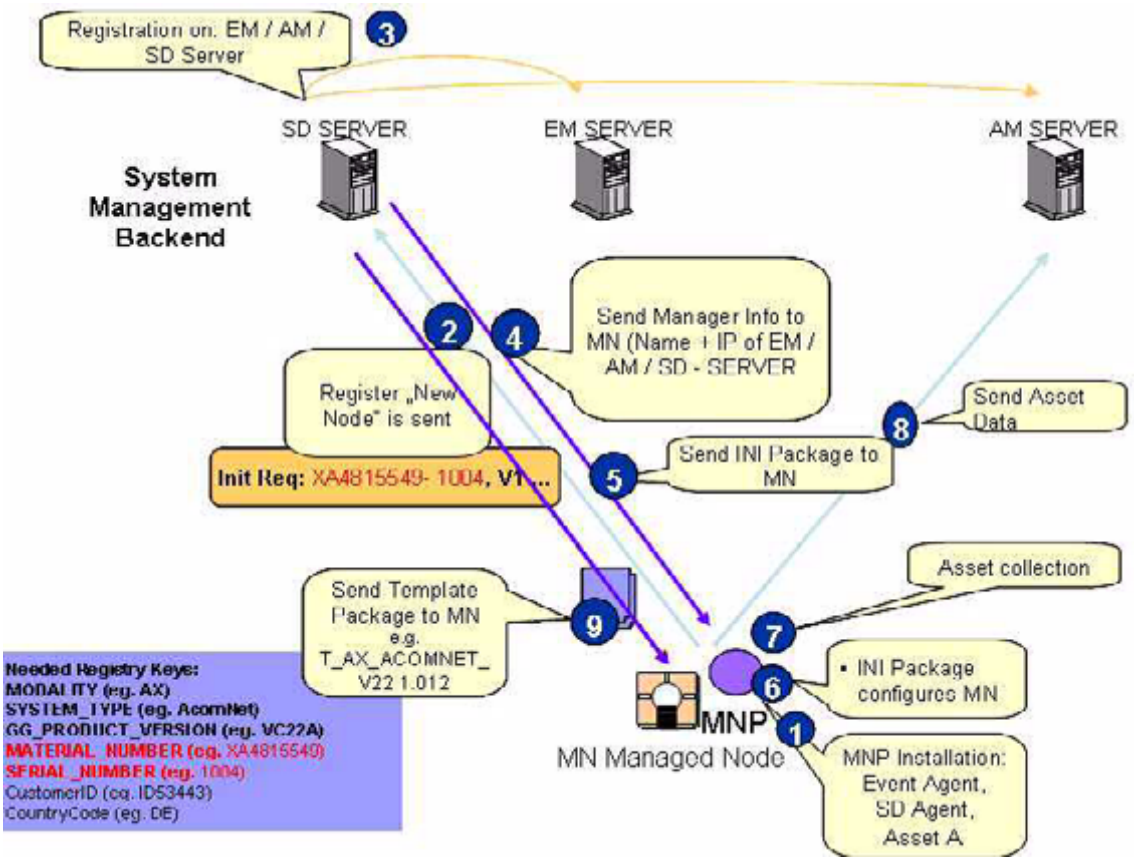

Fig. 28: System management registration

MNP Registration Procedure

The registration procedure starts with a Registration Request.

The Managed Node (MN) sends a set of data which my not be changed afterward, otherwise a data inconsistency avoids a deregistration and a re-registration

- NODE Data Set
- MODALITY (e.g. AX)
- SYSTEM_TYPE (e.g. AcomNet)
- BU_PRODUCT_VERSION (e.g. VC22A)
- MATERIAL_NUMBER (e.g. 4815549)
- SERIAL_NUMBER (e.g. 1004)
- Customer ID (e.g. ID53443)
- Country Code (e.g. DE)

NOTE	**Do not use a zero “0“ at the beginning of a serial or material number.**

Step 1. The CA Unicenter agents are started in the local node.

Step 2. The init request is send to the backend and sends the NODE data set.

Step 3. The backend creates (Build Node DB record) a database record in the software distribution (SD), asset data (AM) and event management (EM) server.

Step 4. The SD server will reply with the name and IP number of the EM and AM servers. The fire wall is now set on the local node (MN).

Step 5. The SD Server will now send the INI package. (For each modality software version, e.g. VC22B, a unique INI Package is stored on the SD server.)

Step 6. The INI package will configure the local node.

Step 7. If the node supports Asset Management, the Asset Collection is done.

Step 8. The asset data will be send to the AM server from now on.

The registration is now complete.

Step 9. The first software distribution is now triggered automatically from the SD server. The first event template will now be sent. This can take up to 15 minutes.

NOTE	**Do not reboot the modality now.**

You can monitor the received template by checking the file `C:\sysmgmt\Template-Version.ini` (e.g. template number 12 received version = T_AX_ACOMNET_VC22 1.012).

MNP Installation/Activation of VGxx Versions

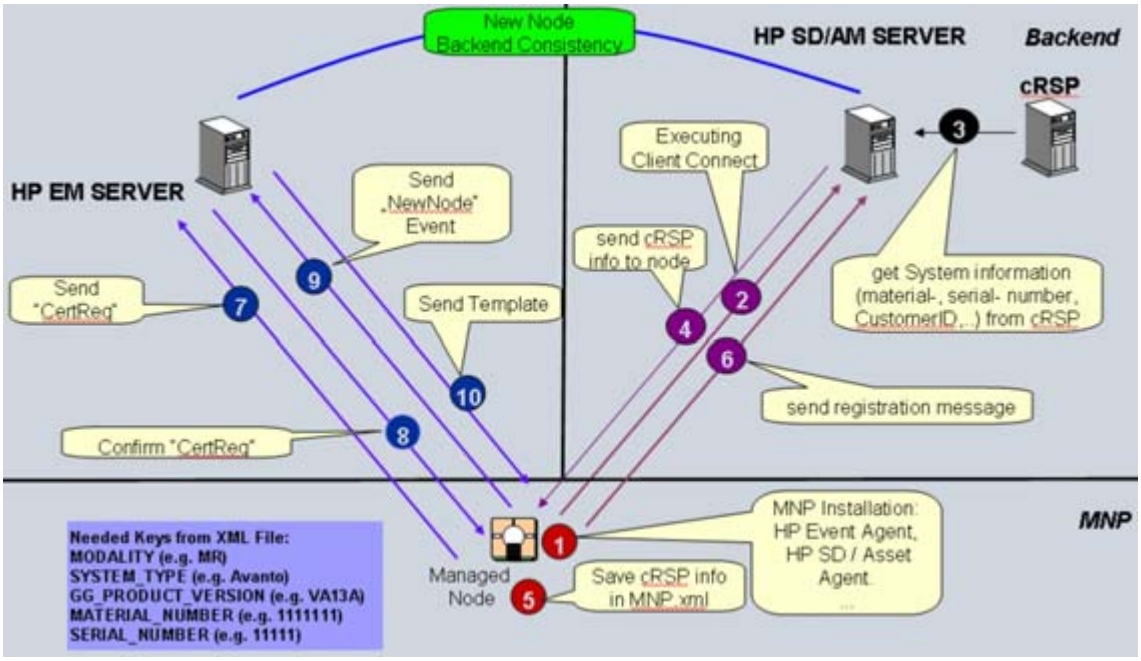

Fig. 29: System Management registration (based on MNP version VGxx)

MNP Registration Procedure

The Managed Node (MN) sends a data set which may not be changed afterwards, otherwise a data inconsistency prevents deregistration and re-registration.

- NODE Data Set
- MODALITY (e.g. AX)
- SYSTEM_TYPE (e.g. AcomNet)
- BU_PRODUCT_VERSION (e.g. VC22A)
- MATERIAL_NUMBER (e.g. 4815549)
- SERIAL_NUMBER (e.g. 1004)
- Customer ID (e.g. ID53443)
- Country Code (e.g. DE)

NOTE	**Do not use a zero “0“ at the beginning of a serial or material number.**

NOTE	**The most important ones are SYSTEM_TYPE and BU_PRODUCT_VERSION. These values are only on the system. The other ones are checked against the values in the SRS portal. Check or let the SRS Help Desk check the values in the SRS portal.**

Step 1. The MNP agent will be installed / activated on the system.

Step 2. The agent sends an Client Connect Request to the SD server.

Steps 3 and 4. The backend gets the data from the SRS portal and sends it to the node.

Step 5. The information is stored in the MNP.xml and compared to the local data.

Step 6 The agent sends the registration message with the NODE data set.

Steps 7 and 8. The agent requests a certificate and gets it from the server to establish a secure connection.

Step 9. The agent sends a “New Node” request to the EM server.

Step 10. The backend (HP EM server) sends the template. (For each modality software version, e.g. VC22B, a unique template is stored on the HP EM server.)

NOTE	**Do not reboot the modality now.**

You can monitor the received template by executing the command **sysmgmt_install -c** in the folder **%MEDHOME%\service\mwtools** or by checking the file **agent_actual_state.xml** in the same folder (e.g. template number 14 received version = 1.014).

TCP/IP Ports

From the Customer System (Modality) to Siemens (DMZ)

VE10 and VF10 (based on CA)

Protocol	Dest. Port	Description
TCP	1721	CCI Remote Daemon
TCP	4105	CA Messaging
TCP	4718 - 4724	Software Delivery
TCP	7001	Common Communication Interface (CCI)
TCP	8222 - 8235	Data Transport Agent (DTA)
TCP	8198	Transfer Object Server
UDP	4104	CA Messaging
UDP	4725	SD Job Check

VF20 (based on CA)

Protocol	Dest. Port	Description
TCP	1721	CCI Remote Daemon
TCP	4105	CA Messaging
TCP	4721	Software Delivery
TCP	7001	Common Communication Interface (CCI)
UDP	4104	CA Messaging
UDP	4725	SD Job Check

VG10 (based on HP)

Protocol	Dest. Port	Description
TCP	8227 see **note 1**	HP Radia Data

Protocol	Dest. Port	Description
TCP	8228 see **note 1**	HP Radia Client Connection
TCP	12061 see **note 2**	HP Event Management

NOTE

Note 1:

In a mixed environment (MNP agents based on VExx/VFxx and VGxx in the same hospital), the HP ports 8227 and 8228 are included in the range of CA ports 8222 - 8235; see (VE10 and VF10 (based on CA) / p. 54).

NOTE

Note 2:

The hospital network administrator must add the ports in the firewall in addition to existing CA ports.

From Siemens (DMZ) to the Customer System (Modality)

VE10 and VF10 (based on CA)

Protocol	Dest.. Port	Description
TCP	1721	CCI Remote Daemon
TCP	4105	CA Messaging
TCP	4718 - 4724	Software Delivery
TCP	7001	Common Communication Interface (CCI)
TCP	8222 - 8235	Data Transport Agent (DTA)
UDP	4104	CA Messaging
UDP	4725	SD Job Check

VF20 (based on CA)

Protocol	Dest. Port	Description
TCP	1721	CCI Remote Daemon
TCP	4105	CA Messaging

Protocol	Dest. Port	Description
TCP	4721	Software Delivery
TCP	7001	Common Communication Interface (CCI)
UDP	4104	CA Messaging
UDP	4725	SD Job Check

VG10 (based on HP)

Protocol	Dest. Port	Description
TCP	8226 see **note 1**	HP Radia notify
TCP	13001 see **note 2**	HP Event Management

NOTE

Note 1:

In a mixed environment (MNP agents based on CA and HP in the same hospital), the HP port 8226 is included in the range of CA ports 8222 - 8235; see (VE10 and VF10 (based on CA) / p. 55).

NOTE

Note 2:

The hospital network administrator must add the ports in the firewall in addition to existing CA ports.

Troubleshooting System Management

If the System Management Configuration completes with an error, the **Status** information displays, e.g, not running (underlined). A pop-up appears when this link is clicked on that provides additional information as shown in (Fig. 30 / p. 57). More detailed information can be obtained in the log files.

NOTE

Following a failed installation and subsequent uninstallation, another attempt should be made to install. Before starting this new installation, contact the SRS Help Desk (Help Desk / p. 76).

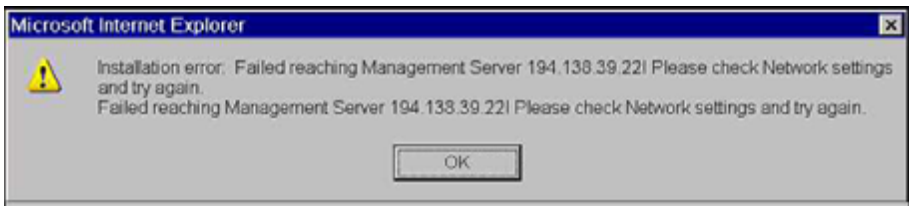
Microsoft Internet Explorer
Installation error: Failed reaching Management Server 194.138.39.22! Please check Network settings and try again.
Failed reaching Management Server 194.138.39.22! Please check Network settings and try again.
OK

Fig. 30: Installation failure

Log Files

Each System Management installation creates a log file of approx. 8-15 KB. A log file is also created if the System Management status is requested via **Local_Service --> Configuration --> SysMgmt --> AgentControls**. In this case, the log file size is approx. 2 KB. The most current log file starts with **sysmgmt_install.log**, followed by **sysmgmt_install_old.log**, and **sysmgmt_install_old_01.log**, etc.

The log files are stored under **%Temp**%, normally c:\Temp.

NOTE

In some systems, the log files can be located in a different directory, see System Troubleshooting.

Description of the Log File, including Corrective Action

Logging Process based on MNP Versions VExx and VFxx

An example of a log file is provided under (Tab. 6 / p. 59). To explain the log file, it has been divided into several configuration steps, indicated by Steps 1 to 7. The corrective action varies, depending on where the error occurred. The example shows an error in configuration Step 5, during download of the INIT package from the server.

NOTE

Check in the log file for the first E = Error in the far left column, because it describes the reason for the failed installation.

Depending on the configuration step, perform the corrective action as described below.

Tab. 5 Explanation of sysmgmt_install.log

Step	Description	Corrective action
1	System Management was started	Information only
2	The medical system connects to the System Management server using port 1721 (CA proprietary protocol).	If the installation fails during this step, check the network connection; it is possible that some ports are closed in the SRS router or it is caused by the customer's firewall. Contact the SRS Help Desk(Help Desk / p. 76) for troubleshooting assistance.
3	Displays the data that are used for registration. Check for the correct serial number, the country, and the Customer_ID.	All data must be filled in. If a blank is entered under, e.g. Customer ID, the System Management installation fails and returns an error at the very beginning of the procedure.
4	Start registration at the System Management server.	Contact the SRS Help Desk if the installation/activation fails during this step.
5	Download the INIT package from the server to the medical system.	Most installations fail during this step. If so, repeat the installation once. Contact the SRS Help Desk if the installation fails again.
6	Automatic rollback is started if the installation fails	Information only (available from MNP VF10 onwards)
7	Status of System Management Installation	Information only

Tab. 6 Example of sysmgmt_install.log

I	11/09/2006	09:23:31	**********
I	11/09/2006	09:23:31	System Management Managed Node Package, Version VF10F(3.19)
I	11/09/2006	09:23:31	**********
I	11/09/2006	09:23:31	OS=Win2003
I	11/09/2006	09:23:31	READ IN THE OPTIONS

.....

Step 1: Start installation and activation of System Management

I	11/09/2006	09:23:35	START Installation of System Management Base (Offline 2. Part)
I	11/09/2006	09:23:35	START enable of all CA Communication services END enable of all CA services Communication IP=192.168.186.116
I	11/09/2006	09:23:36	Check for valid IP address of Manager

Step 2: Connectivity check

I	11/09/2006	09:23:37	Check whether Management Server is reachable. (timeout: 300 sec.) Scanning: e.g., 194.138.39.22 port 1721. Management Server 194.138.39.22 successfully reached
I	11/09/2006	09:23:37	----------

Step 3: Registration data

I	11/09/2006	09:23:37	This is an example for Sensation 64 with serial # 54777 and Navigator IP 192.168.186.116, located in Germany WSNAME= ct_neuro Node_IP = 192.168.186.116 Node_Name = CT8377520-54777 Host Name = ct_neuro Host IP = 192.168.186.116 Modality = CT System_Type = P30F Product_Version = VB30A Serial Number = 54777 Material Number = 8377520 CUSTOMER_ID = ID COUNTRY = DE
I	11/09/2006	09:23:37	START Installation of System Management Base

I 11/09/2006 09:23:37 START Modify of etc./Hosts File

Successful entry in hosts file

END Modify the etc/Hosts File

START setting of system variables

Successful setting of system variables

END Setting of system variables

Step 4: Start Registration with server

I 11/09/2006 09:23:41 Check whether Management Server is reachable. (timeout: 300 sec.)

Scanning: e.g. 194.138.39.22 port 1721

Management Server 194.138.39.22 successfully reached

I 11/09/2006 09:23:44 Registering the node: CT8377520-54777 with Manager 194.138.39.22 with message =[c:\sysmgmt\TND\BIN\cawto -n 194.138.39.22 -s CT8377520-54777 "New Node: CT8377520-54777 App: CT_P30F_VB30A Site: DEn.a. SourceIP: e.g. 192.168.186.116 " > C:\DOC-UME~1\ADMINI~1\LOCALS~1\Temp\log\cawto.txt 2>&1]

I 11/09/2006 09:23:45 Successful registration with server

END registration with server

.....

Step 5: Download INIT package from server

I 11/09/2006 09:25:25 START init of the node

I 11/09/2006 09:25:25 Wait up to 15 minutes for INIT of the node

E 11/09/2006 09:40:25 Failed init of the node:

.....

Step 6: Automatic rollback if activation of System Management failed

I 11/09/2006 09:40:25 START Automatic Rollback from System Management

.....

I 11/09/2006 09:41:26 END Automatic Rollback from System Management

Step 7: Status of System Management Installation/Activation

E 11/09/2006 09:41:30 Failed installation of System Management Base (failed init of the node:)

Logging Process based on MNP Version VGxx

An example of a log file is provided under (Tab. 6 / p. 59). To explain the log file, it has been divided into several configuration steps, indicated by Steps 1 to 6. The corrective action varies, depending on where the error occurred. The example shows an error in configuration Step 3, during Start Registration Data.

Tab. 7 Explanation of sysmgmt_install.log

Step	Description	Corrective action
1	System Management was started	Information only
2	The medical system connects to the System Management server using port 8228 (HP proprietary protocol).	If the installation fails during this step, check the network connection; it is possible that some ports are closed in the SRS router or it is caused by the customer's firewall. Contact the SRS Help Desk (Help Desk / p. 76) for troubleshooting assistance.
3	Displays the data that are used for registration. Check for the correct serial number, the country, and the Customer_ID.	All data must be filled in. If a blank is entered under, e.g. Customer ID, the System Management installation fails and returns an error at the very beginning of the procedure. **If you don't know the correct values, you have to enter dummy values for country or customer ID**. These values will be replaced at the backend by the synchronization with the SRS portal
4	Start registration at the System Management server.	Contact the SRS Help Desk if the installation/activation fails during this step.
5	Download the template from the server to the medical system.	Contact the SRS Help Desk if the installation fails during this step.
6	Status of System Management Installation	Information only

Tab. 8 Example of sysmgmt_install.log

I	02/28/2008		**********
I	02/28/2008	10:27:40	System Management Managed Node Package - Version VG10A (4.00)
I	02/28/2008	10:27:40	**********
I	02/28/2008	10:27:40	OS=WinXP/.Net Service Pack 2 (Version: 5.1 Build: 2600 Type: X86-based PC)
I	02/28/2008	10:27:40	READ IN THE OPTIONS

.....

Step 1: Start installation and activation of System Management

I	02/28/2008	10:27:40	START Installation of System Management Base
I	02/28/2008	10:29:25	HPSD installed
			HPEA installed
I	02/28/2008	10:29:53	Check for valid IP address of Manager (SD)
I	02/28/2008	10:29:53	Check for valid IP address of Manager (EM)

Step 2: Connectivity check

I	02/28/2008	10:29:53	Check whether the Management Server is reachable. (time-out: 120 sec.)
			Management Server successfully reached 194.138.36.82
I	02/28/2008	10:29:53	----------

Step 3: Registration data

I	02/28/2008	10:29:55	This is an example for an Artis with serial # 135101 located in Germany (Release Environment)
			WSNAME = AXISCSAX
			Node_IP =
			Node_Name = XA10094135-135101
			Host Name = AXISCSAX
			Host IP =
			Modality = XA
			System_Type = Artis dF
			Product_Version = VC12C
			Serial Number = 135101
			Material Number = 10094135
			CUSTOMER_ID = Id
			COUNTRY = DE

I 02/28/2008 10:29:55 START Modify of etc./Hosts File

Successful entry in hosts file (SD Server)

Successful entry in hosts file (EM Server)

I 02/28/2008 10:29:55 START configuration/registration of Sofware Delivery / Asset Agent

Read MNP.XML (Backend Sync = true)

****

If the “Backend Sync = false”, the agent did not get the data from the backend to synchronize it with its locally stored data

****

Step 4: Start Registration with server

I 02/28/2008 10:31:11 START configuration/registration of Event Agent

START configuration of Event Agent

START starting the Event Agent

START Installation of Certificate

Successful installation of Certificate

****

This is an important step. If it fails, call the SRS Help Desk.

****

START Import of Basic Policies (REL)

Successful Import Basic Policies of Event Agent (0 Retr)

START Send New Node Event)

Send Event: "c:\sysmgmt\EMAgent\bin\opcmsg.exe" application=SRS_NodeAgt object=AX10094135-135101 msg_grp=NewNode msg_text="CORE_ID: 1a16d972-1086-752d-0999-c69c8d62548c MODALITY: AX SYSTEM_TYPE: Artis dF PRODUCT_VERSION: VC12C MATERIAL_NO: 10094135 SERIAL_NO: 135101 COUNTRY: -Test CITY: Forchheim SITE: TD-PS-21" node=REL-HP

Step 5: Download Template from server

I 02/28/2008 10:35:28 START Installation of Template (waiting up to 5 minutes)

I 02/28/2008 10:37:11 Successful Installation of Template (Template Version = 1.03)

I 02/28/2008 10:37:11 START starting the services

.....

Step 6: Status of System Management Installation/Activation

I 02/28/2008 10:38:01 Successful installation of System Management Base

General Information regarding System Management

How to deactivate or uninstall System Management

Uninstallation of the System Management from VF10 onwards is not necessary due to the implemented rollback functionality. In other words, if the installation detects an error, the software is rolled back automatically. If the installation is successful, there is no need for uninstallation.

- Deactivation of System Management

  Disable the System Management Base - **Activated** checkbox and press **<Go>** to deactivate the System Management. All services are stopped, System Management is deactivated. In this status, System Management does not use any system resources.

- Uninstalling System Management

  Disable both System Management **Activated** and **Installed** checkboxes and press **<GO>**. The System Management software is rolled back completely.

NOTE	**Please use the routine described above for the uninstallation, otherwise reinstallation will fail.**

System Management Backup/Restore Strategy

System Management is fully backed up (Backup/Restore) in medical systems. If the software reinstallation is performed with backup/restore, the System Management Configuration is executed automatically upon restore. This will extend the restoration time by approx. 8-10 minutes if the configuration succeeds, or even longer if it fails.

System Management Pop-ups

The following is a list of pop-ups that have appeared during the software integration and test phase. The pop-ups appeared during software installation, including restore or in regard to installation or uninstallation of System Management. The pop-ups had no functional effect.

1. **Another System Management action is running already**

   During software startup, Syngo checks the actual and the desired status of System Management. If both do not match, the configuration is started automatically.

   When checking the System Management status under **Local_Service --> Configuration --> SysMgmt --> AgentControls**, a message may be displayed indicating that another System Management installation is already running. This message may appear during software update, or when restoring the system tables (SW settings include the System Management configuration file).

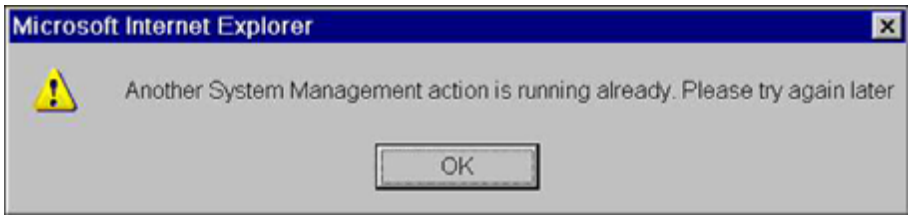

Fig. 31: Another_SystemManagement_running

   Wait a maximum of 15 minutes and check again.

2. **tngboot.exe**

   This pop-up may appear only during installation. It indicates that the System Management Offline installation was not performed correctly during software installation.

Fig. 32: CA_Offline_Popup

3. **wtsutil.dll**

   After the final configuration of System Management and before a system reboot (reboot is not required in the installation routine for VF10 or higher), some path variables have not yet been updated. If at that time an escalation is triggered by the system due to, e.g. too many restarts or continues, the following pop-up will appear. Once the system is rebooted after the System Management Installation, the following pop-up will not appear.

CAWTO.EXE - Unable To Locate Component
This application has failed to start because wtsutil.dll was not found. Re-installing the application may fix this problem.
OK

Fig. 33: CA_Popup

4. **Agent_send**

   The pop-up Agent_Send appeared once in the field during restore. It had to be acknowledged to continue.

5. **radia.vbs**

   This pop-up may appear after a failed installation and the required reboot during the next installation attempt. There is no problem, just a run-key of the old installation, which can not be executed at this time. Later in the installation process, the run-key will be activated again and successfully executed. So you just need to click on **Ok** here

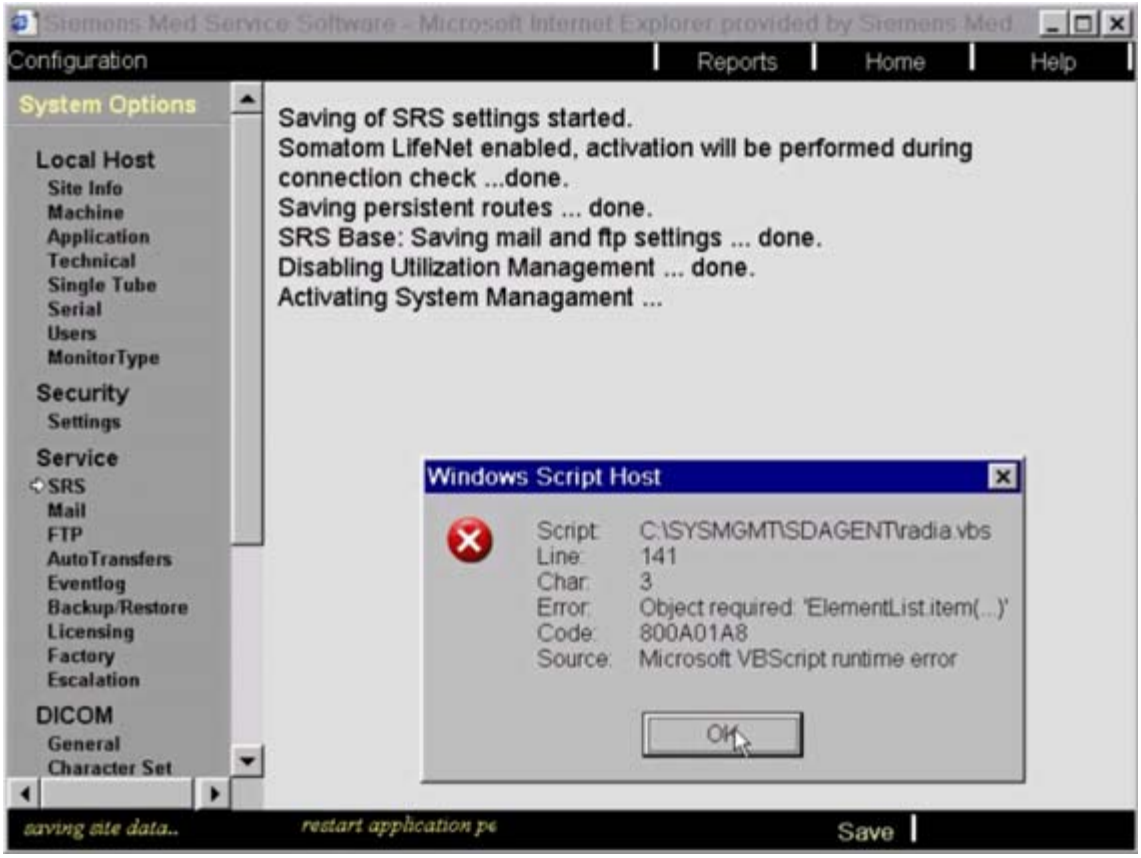

Fig. 34: HP_reinstallation_pop-up

System Management Installation Check

Following System Management installation, the system requires a template from the server whereby the System Management Installation is completed. Depending on the connection, this can take up to 30 minutes.

- Open a command window; for details, refer to the system instructions.
- In the command window, enter **%medhome%\service\mwtools\sysmgmt_install.exe -c** ↵ and confirm with Return.
- If the MNP Version is VGxx any Filter Version is ok, but if it is missing, a new registration is necessary.

- If the MNP Version is VExx of VFxx, the version of the template sent by the System Management server must be ≥**1.010**. If this is not the case, the installation failed and the SW must be uninstalled.(How to deactivate or uninstall System Management / p. 64). Contact the SRS Help Desk for troubleshooting (Help Desk / p. 76).

  This can be read out under **Rules/Filter Version**

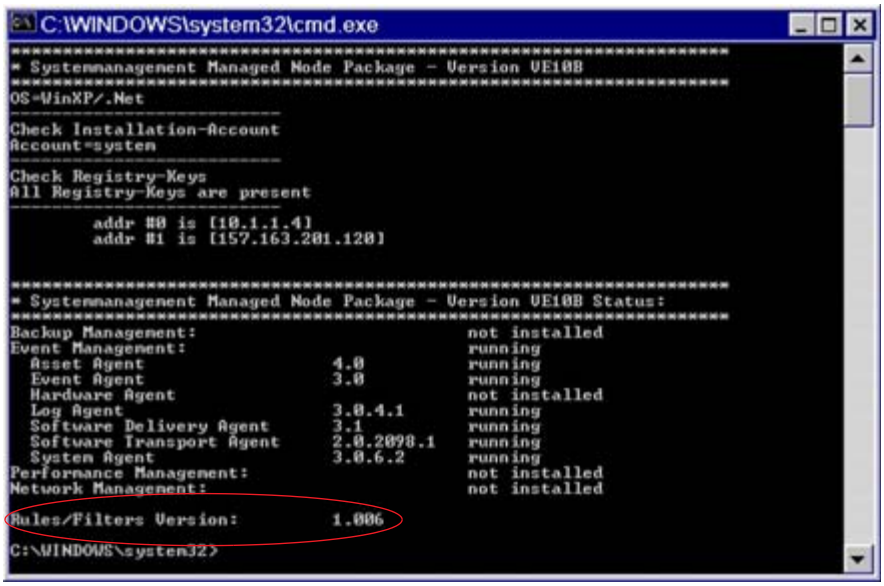

Fig. 35: Template version

This information is also logged in the log file **%temp%\sysmgmt_install.log**

System Management Connectivity Check

This function is available in **Syngo VE31C** or higher and with **agent_desired_state.xml** version 2.4 or higher.

Fig. 36: Version Agent_desired_state.xml

- System Management must be activated and must function.
- Open a Notepad and edit the **agent_desired_state.xml** from the directory **%med-home%\service\mwtools**.
- The xml interface version must be 2.4 or higher.
- Go to the section **<REQUIREDACTIONS>**
- Change the value in the key `<SYSTEMMANAGEMENTCHECK>false</SYSTEMMAN-AGEMENTCHECK>` from **false** to **true**.
- **Save** the new settings

- Open a command window; for details refer, to the system instructions.
- In the command window, enter **%medhome%\service\mwtools\sysmgmt_install.exe -x** ↵ and confirm with Return.
- Change the key `<SYSTEMMANAGEMENTCHECK>true</SYSTEMMANAGEMENTCHECK>` back to **false**.
- Go to the directory c:\sysmgmt and look in the result of the log file: **SystemManagementBaseCheck.log**.

Tab. 9 Example of SystemManagementBaseCheck.log

05/30/07	09:44:16	START the System Management Base connection test
05/30/07	09:44:18	Connection test message received locally, executing local reaction ...
05/30/07	09:44:20	Message sent to local event agent successfully.
05/30/07	09:44:20	Now sending a test message to the event manager: FTHW9MTA
05/30/07	09:44:27	Message send.
05/30/07	09:44:28	Waiting for manager response ...
05/30/07	09:44:30	SUCCESS: Manager response received
05/30/07	09:44:32	Now sending response result to the manager: FTHW9MTA
05/30/07	09:44:32	SUCCESS: Response result sent successfully.
05/30/07	09:44:32	SUCCESS: System Management Base connection is fully operational at the moment.
05/30/07	09:44:33	END System Management Base connection test

Remote Update Handling / Software Distribution

Update Handling can fail for a number of reasons..

- The system logged on to the software distribution server with another serial or material number than is entered in the RDiag.
  - Compare the entries in the system with those in the RDiag.
  - Register the system again in System Management with the correct combination of part and serial number (Site Identification / p. 13).

- System Management is not or is incorrectly installed on the system.
  - Reinstall System Management.

- The system is registered on the software distribution server with the incorrect IP address.
  - Compare the IP address to the one in the RDiag.
  - Register the system again in System Management.

- SD GUI not distributed on the system.

NOTE	**Systems with syngo VE30 or higher have a built-in SD GUI.**

  - Contact the SRS Help Desk to determine whether the SD GUI can be downloaded manually.
  - Register the system on the System Management server again to obtain the SD GUI automatically.
  - The patch level of the system software for the SD GUI is not known on the software distribution server. Initiate clarification from the SRS Help Desk so that the patch level in the server is known.

NOTE	**The SD GUI is distributed only for systems which are connected to SRS via a VPN broadband connection.**

  SD GUI distribution can take up to 3 days.

- The MNP ports may be closed by customer administrator.

Virus Protection

Prerequisites

The following tasks are necessary for Installation / Configuration of Virus Protection:

- The setup for SRS and System Management must have been performed and must be operable.

NOTE	**System Management is a basic functionality in medical system.** **It should be configured even if virus protection is not ordered by the customer.**

- For syngo version < VE30A and non-syngo systems (e.g FLUOROSPOT COMPACT), the CS SD GU 3.x is installed.

NOTE	**Check for sd_gui directory under c:\<%MEDHOME%>\service\mwtools. If available, the SD GUI is correctly installed at the system.** **If not available, contact the SRS Help Desk and request it.**

- The customer has ordered the virus protection service.
- The Installation or Upgrade DVD is available or the virus scanner is pre-configured and disabled.

NOTE	**If the virus scanner exists on the system and is disabled, no pattern file may exist** **(with existing pattern file --> license problem).**

- The local service organization triggers the enabling process.
- A CSE is at the customer site to install and configure the virus protection.

Downloading the latest Pattern Files

Today, a new virus pattern update is required to check the functionality. Since this may take approx. 1-2 days, contact the SRS Help Desk and request the download of a new virus pattern file.

During system restart, the SD GUI is displayed informing the user about the new virus pattern update.

In systems with syngo VE30 or higher, an icon appears during normal work to indicate to the customer that a virus pattern update is available. After a reboot, the SD GUI also appears.

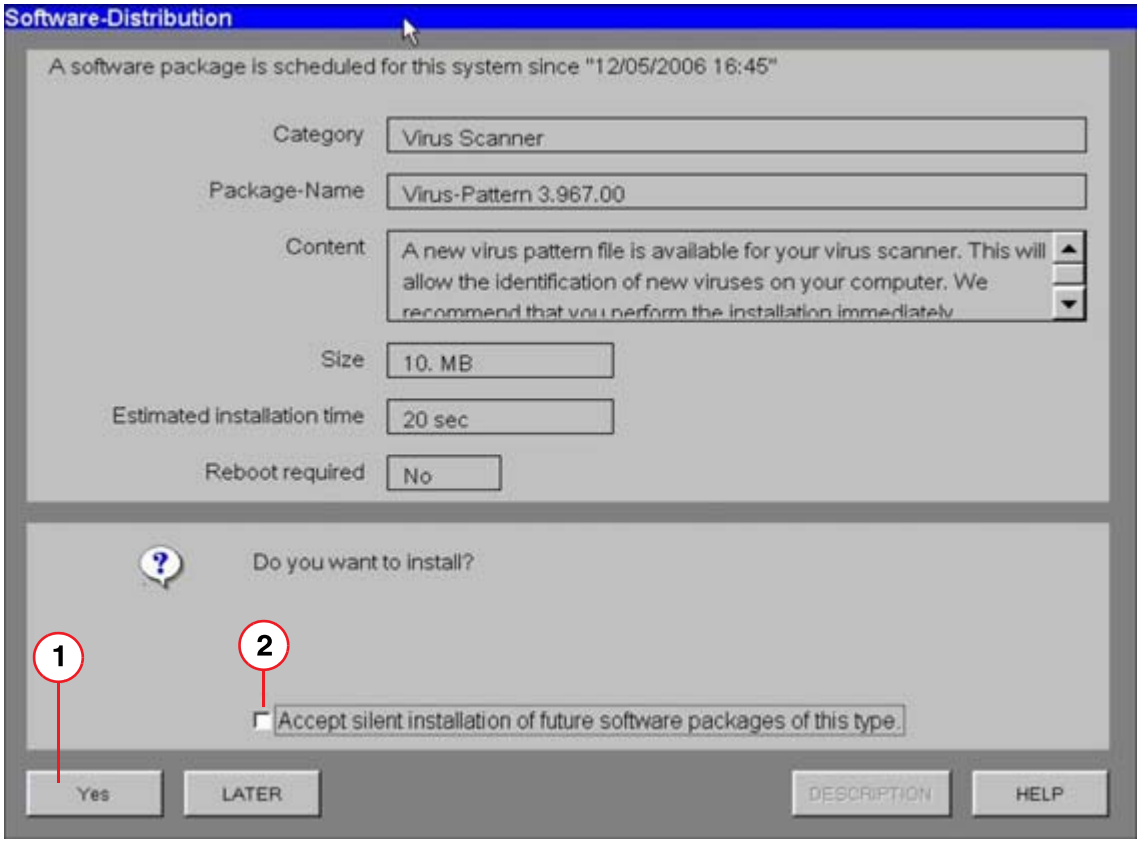

Fig. 37: Window of CS SD GUI

Pos. 1 Click “Yes” to start installation

Pos. 2 When the checkbox is checked, the next packages of the “Virus Scanner” category will be installed in silent mode.

The virus pattern is installed by clicking on “Yes”, see position 1 in the figure.

Tab. 10 Definition of Buttons in the SD GUIs

SD GUI	Syngo built-in SD GUI
YES	Install
Later	Defer / Defer all

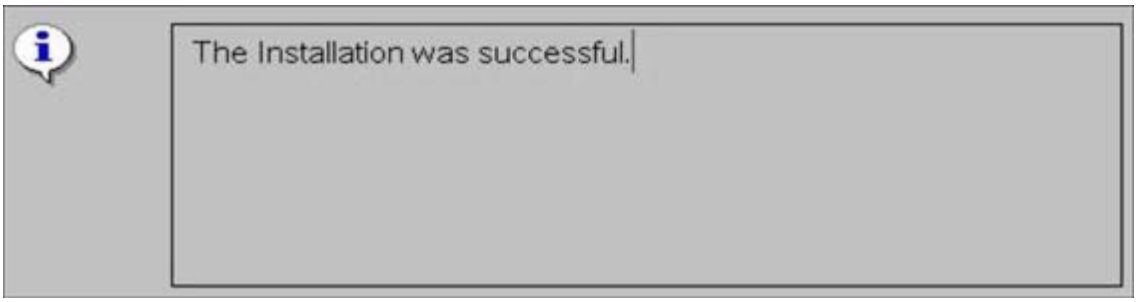

Fig. 38: CS SD GUI successful message after the installation of a software package

This window will appear with the next reboot by clicking on the “LATER” button. The dialog box closes without performing the installation.

If the installation has failed for any reason, a corresponding message will be displayed. In this case, information regarding the failed installation will be automatically forwarded to your Siemens UPTIME Service Center for resolution. For faster support at the customer's location, call directly: SRS Help Desk.

The following steps are performed by activating the checkbox, see position 2 in the figure:

- The next software packages (for e.g. virus pattern with the category “Virus Scanner”) will be installed in the silent mode.

NOTE	**With the next virus pattern, the CS SD GUI will not be displayed** **--> the virus pattern update runs in the background without any user action.**

- The file unattended.ini is created in the directory

  c:\%MEDHOME%\service\mwtools\sd_gui.

L.	Contents of unattended.ini	Comment
1	[CS_Virus Pattern]	Section package, category 1 --> Virus Pattern
2	Display GUI=false	For the next virus pattern, the CS SD GUI is not displayed for the user. The virus pattern is installed silently.
3	Command Visible=false	
4	[CS_Microsoft-Hotfixes-XP-EN-SP2]	Section package, category 2 --> Microsoft Hotfixes XP EN SP2
5	Display GUI=false	For the next virus pattern, the CS SD GUI is not displayed for the user. The virus pattern is installed silently.
6	Command Visible=false	
7	[Automatic Package Install]	Section list of all available packages
8	Package 1=CS_Virus Pattern	
9	Package 2=CS_Microsoft Hotfixes-XP-EN-SP2	

Perform the following to make the CS SD GUI visible for the software package category “CS_Virus-Pattern”:

- delete the unattended.ini if only one package category entry exists or
- rename the string “Package2” to “Package1” in line 9
- delete the lines 1, 2, 3 and 8

Checking the Functionality of Software Distribution of the Virus Pattern (silent mode)

In the silent mode (without pop-up window of CS SD GUI), you will not know which version of the virus pattern is actually downloaded.

To see the current version of the virus pattern that is downloaded, check the two directories as shown:

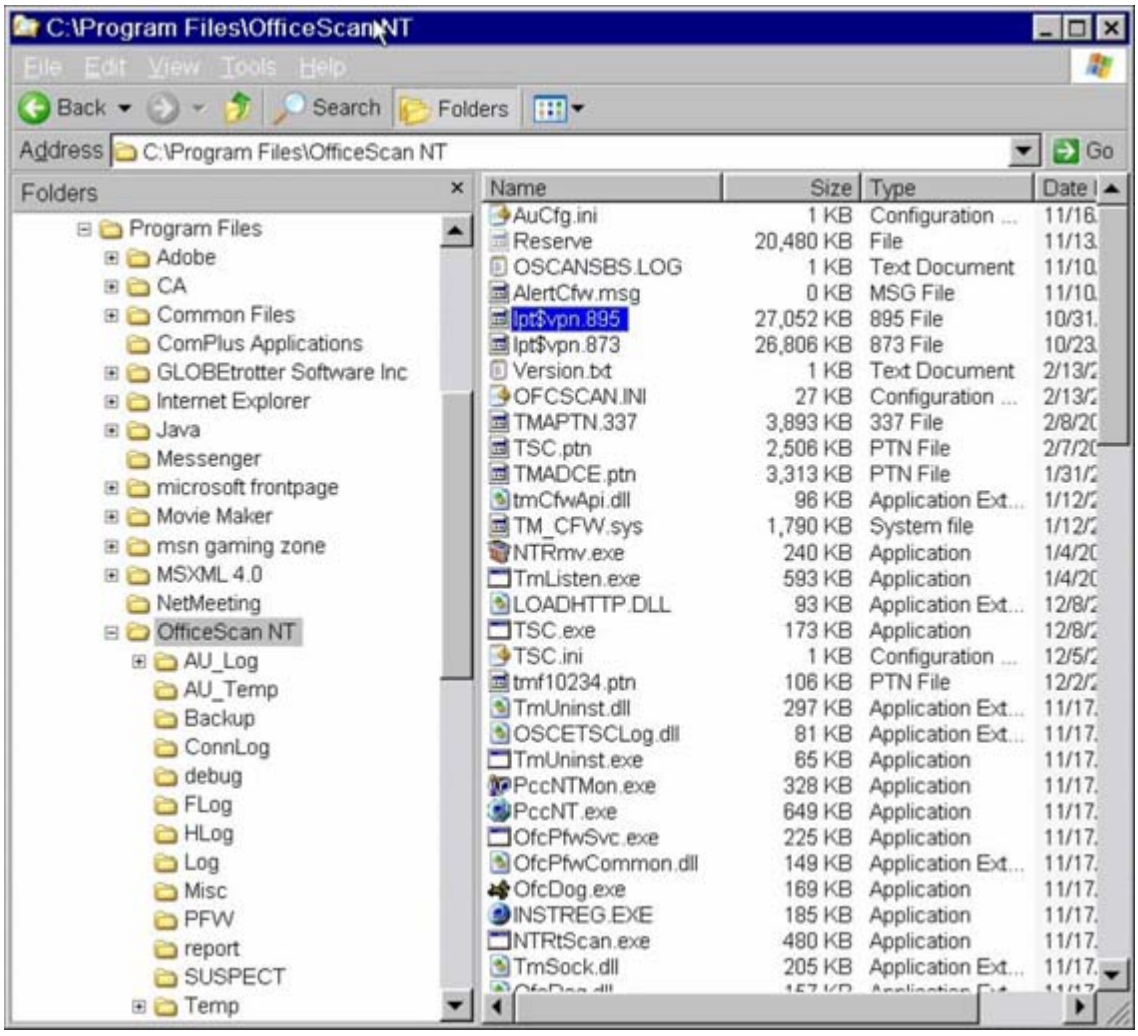

Fig. 39: Trend Micro location of the complete download of a virus pattern

You will need administrative rights for this check:

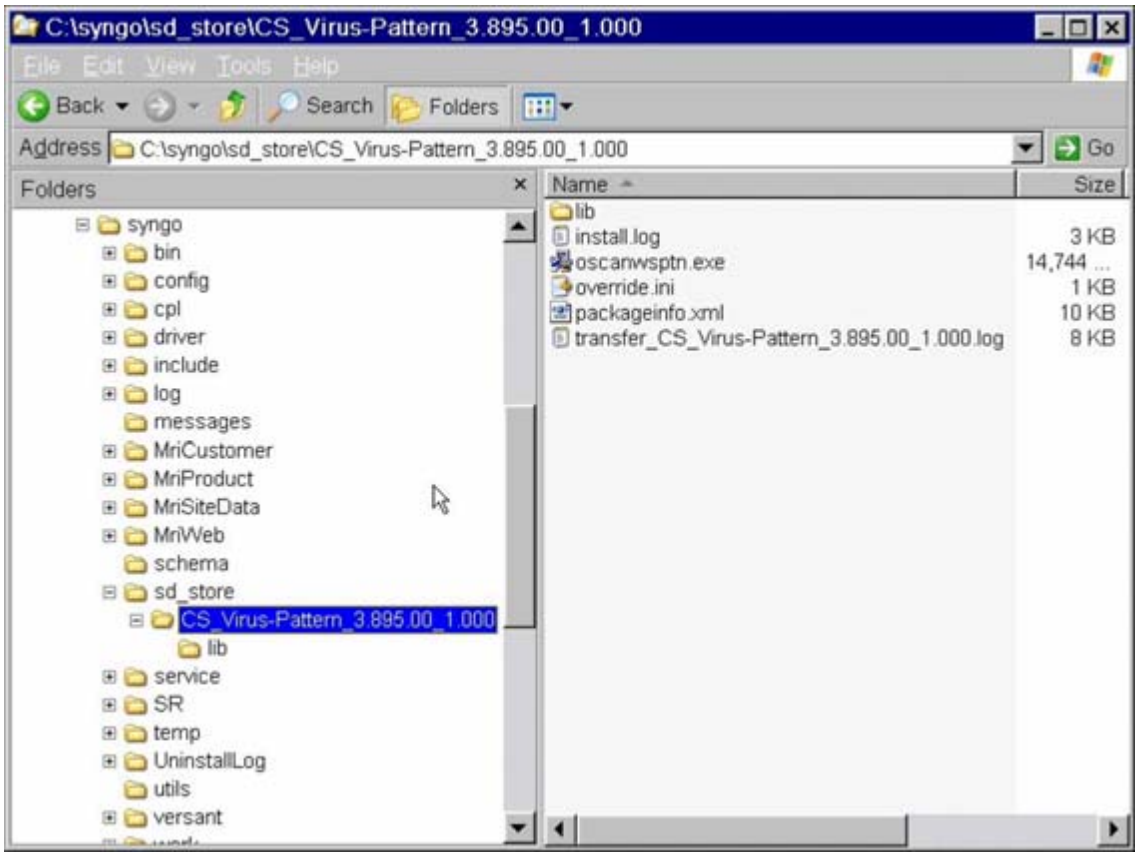

Fig. 40: MNP location of the complete download of a virus pattern

Help Desk

If there are any questions or any problems, please contact the following Help Desk:

- SRS Help Desk **worldwide**
  Phone: +49 919118 8080 CODE 1-9-1
  Fax: +49 9131 84 13 7388
  E-Mail: RemoteServer.med@siemens.com
  Service days: Monday - Friday
  Service hours: 7:00 AM - 10:00 PM CEST (German time)

- SRS Help Desk (**USA only**)
  Phone: +1 800 576 7336 CODE 2-3-13
  E-Mail: csg.srs.med@siemens.com
  Service days: Monday - Friday
  Service hours: 8:30 AM - 7:00 PM EST

SRS Toolkit

The toolkit is available on the **Intranet**; see the **CS home page**:

-> For Service -> Product Information -> Siemens Remote Service -> CB-DOC

Final Configuration Checklist

The **SRS checklist** is available on the **Intranet**; see the **CS home page**:

-> For Service -> Product Information -> Siemens Remote Service -> CB-DOC ->

-> Installation -> System -> Installation Instructions -> SRS Final Configuration Checklist

The checklist can be sent directly to: Srs_final.med@siemens.com

Alternatively by fax: +49 9131 84 13 7388

Router Order Form

The **router order form** is available on the **Intranet**; see the **CS home page**:

-> For Service -> Product Information -> Siemens Remote Service -> CB-DOC ->

-> Planning -> System -> Planning Guide -> Router order form

Send the router order form back via fax: +49 9131 84 8835

Pre-Connect Tool (download)

The SRS Pre-connect Tool is available on the **Intranet**; see the **CS home page**:

-> For Service -> Product Information -> Siemens Remote Service -> CB-DOC ->

-> Installation -> System -> Installation Instructions -> Pre-connect Tool

-> A description of the Pre-connect Tool also can be found at that location.

Siemens Remote Portal Access

A personal account is required on the SRS portal to access data and to connect to systems.

For accounts, see “Contact MMD Country Admin”:

http://cs.med.siemens.de/cms/en/tools/mmdcountryadmin/default.asp

Knowledge Base / Life Net

Prerequisites

To obtain access to the Knowledge Base and Life Net, a SRS connection must have been performed and must be operable.

For more details, please refer to the system configuration instructions for Siemens Remote Service.

NOTE	**Systems with Syngo VE31C and higher have access to the Knowledge Base in the Help menu in the service software.**

Making sure that you have an SCD Account and Password on the Siemens Intranet

If you have forgotten your password in SCD or do not know where you can get this password, start with the following steps:

1. Start the SCD WEB Application on the Intranet and choose your own account
   e.g Frank Urban (Fig. 41 / p. 79).

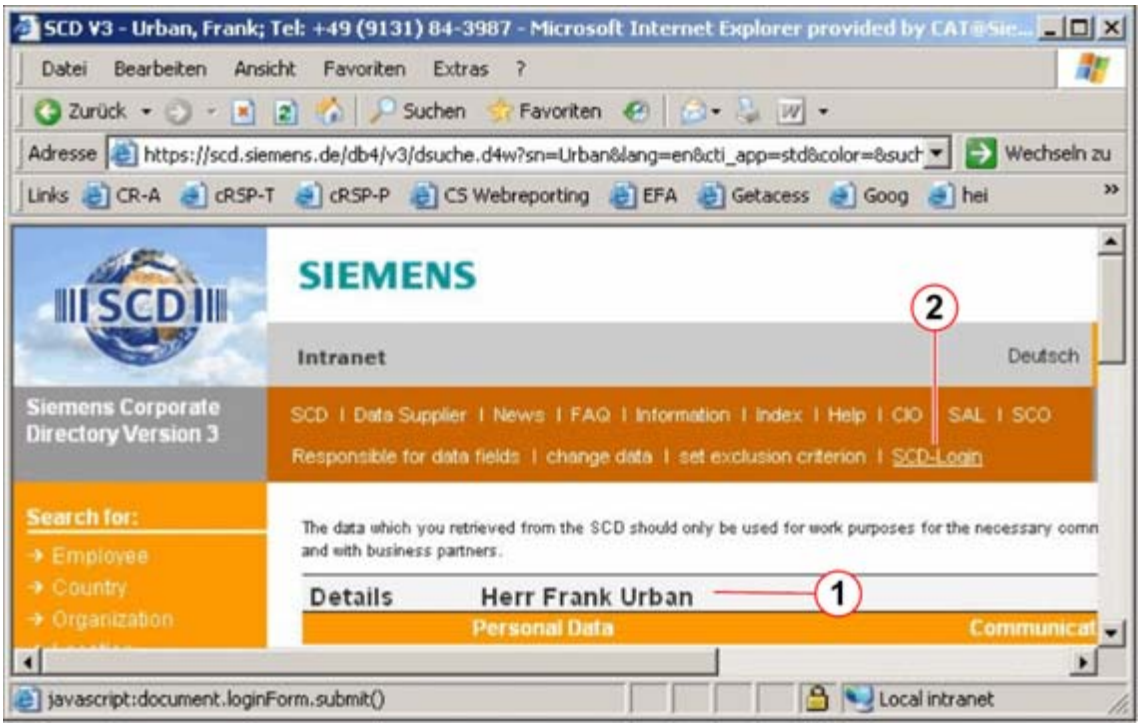
SCD V3 - Urban, Frank; Tel: +49 (9131) 84-3987 - Microsoft Internet Explorer provided by CAT@Sie...
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse https://scd.siemens.de/db4/v3/dsuche.d4w?sn=Urban&lang=en&cti_app=std&color=8&suc
Wechseln zu
Links CR-A cRSP-T cRSP-P CS Webreporting EFA Getacess Goog hei
SCD
SIEMENS
Intranet
Deutsch
Siemens Corporate Directory Version 3
SCD | Data Supplier | News | FAQ | Information | Index | Help | CIO | SAL | SCO
Responsible for data fields | change data | set exclusion criterion | SCD-Login
Search for:
Employee
Country
Organization
The data which you retrieved from the SCD should only be used for work purposes for the necessary comm
and with business partners.
Details Herr Frank Urban
Personal Data
Communicat
2
1
javascript:document.loginForm.submit()
Local intranet

Fig. 41: Set password in SCD - part 1

2. Click on (2/Fig. 41 / p. 79) to start the request process.
   ➪ The following page will be displayed.

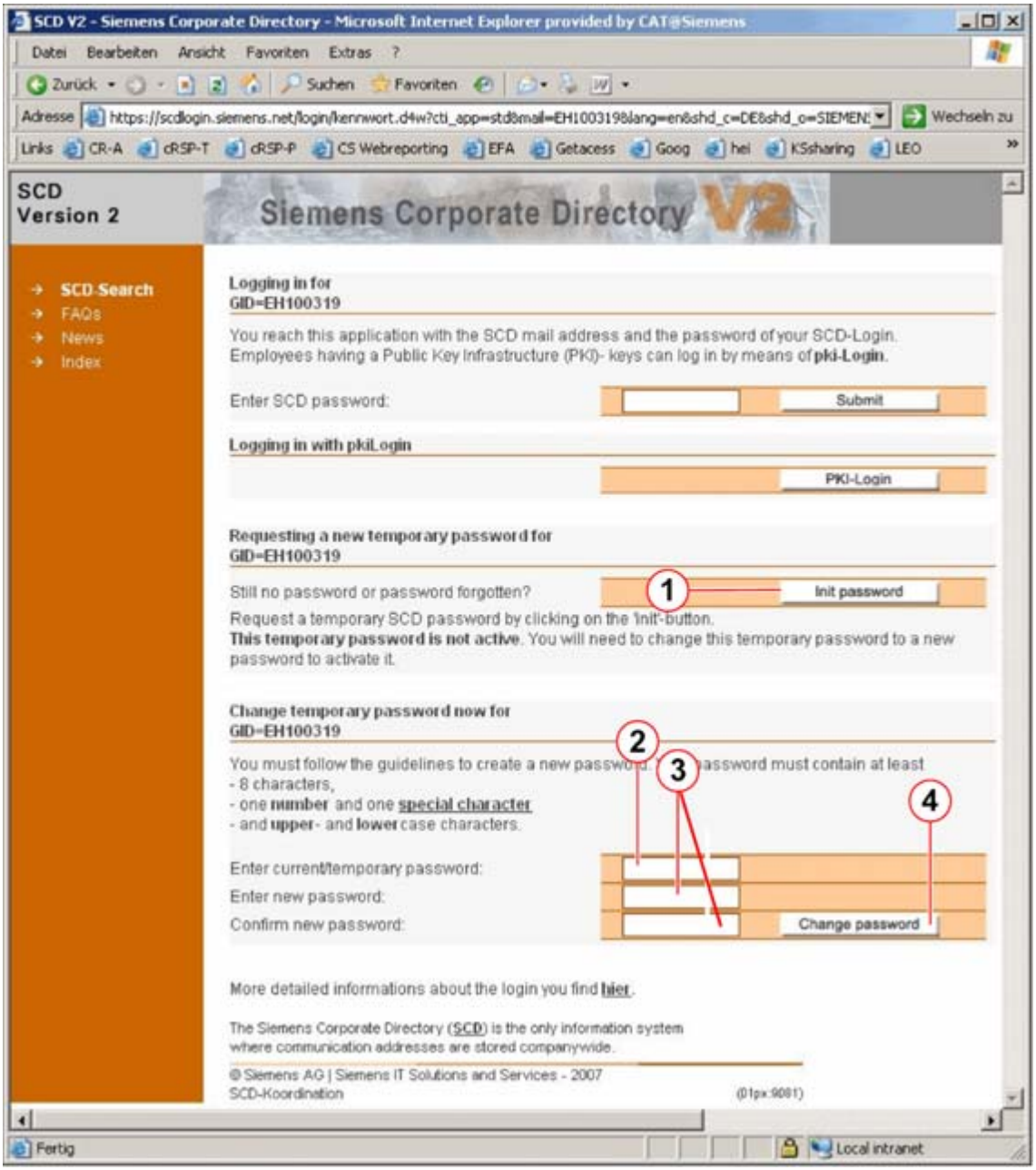
SCD V2 - Siemens Corporate Directory - Microsoft Internet Explorer provided by CAT@Siemens
SCD Version 2
Siemens Corporate Directory V2
SCD-Search
FAQs
News
Index
Logging in for GID=EH100319
You reach this application with the SCD mail address and the password of your SCD-Login.
Employees having a Public Key Infrastructure (PKI)- keys can log in by means of pki-Login.
Enter SCD password:
Submit
Logging in with pkiLogin
PKI-Login
Requesting a new temporary password for GID=EH100319
Still no password or password forgotten?
Init password
Request a temporary SCD password by clicking on the 'init'-button.
This temporary password is not active. You will need to change this temporary password to a new password to activate it.
Change temporary password now for GID=EH100319
- 8 characters,
- one number and one special character
- and upper- and lower case characters.
Enter current/temporary password:
Enter new password:
Confirm new password:
Change password
More detailed informations about the login you find hier.
The Siemens Corporate Directory (SCD) is the only information system where communication addresses are stored companywide.
© Siemens AG | Siemens IT Solutions and Services - 2007
SCD-Koordination
1
2
3
4

Fig. 42: Set password in SCD - part 2

3. Click on (1/Fig. 42 / p. 80) to request an init password.
   ➪ The init password will be sent to your mailbox.
4. Open your mailbox and look in your input folder for the temporary password.
5. Put this temporary password in (2/Fig. 42 / p. 80).
6. Generate a new password in (3/Fig. 42 / p. 80).
7. Click on (4/Fig. 42 / p. 80) to activate the new password.
   ➪ Use this new password for access to the new KB.

Accessing the CS Knowledge Base for Systems without syngo or syngo lower than VE31C

NOTE	**The account and password from SCD is used for the new Knowledge Base, see (Prerequisites / p. 79).**

NOTE	**There is a new link to the KB:** **https://smskb.medical.siemens.com/selfservice**

Opening the Internet Explorer

- Select **Windows Explorer**.
- Select **Iexplore.exe** in the path `c:\program files\Internet Explorer`.

Internet Explorer Settings

- Click on the **<Tools>** menu in the header of the Internet Explorer Window and then select **<Internet Options>**. The `Internet Options` window will open.
- Select the “Connections“ tab card.

Fig. 43: Internet Options

- Click on **LAN Settings** in the Local Area Network (LAN) settings box.

Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 194.138.39.18
Port: 8080
Advanced...
Bypass proxy server for local addresses
OK
Cancel

Fig. 44: LAN settings

- Select the **<Use a proxy server for your LAN (these settings will not apply to your dial-up or VPN connections)>** checkbox and `Proxy Server`.
- Get the **Address** and **Port** from the table below and enter them.

Input location	Input
Address	**Enter the IP address** according to the SRS server already used: **194.138.39.18** for **Europe**, or **129.73.116.92** for **USA**, or **194.138.243.178** for **Asia**.
Port	**8080**

- Select the **<Bypass proxy server for local addresses>** checkbox.
- Under `Proxy Server`, press **Advanced.**

Fig. 45: Proxy settings

- Under `Exceptions - Do not use proxy server for addresses beginning with`, enter **<10.1.1.*>**.

- Click on **OK** to close the “Proxy Settings“ window.
- Click on **OK** to close the “Local Area network (LAN) Settings“ window.
- Click on **OK** to close the “Internet Options“ window.

Connecting to the CS Knowledge Base

- Enter **https://smskb.medical.siemens.com/selfservice/** ↵ in the address line. Establishment of the network connection is started.

KNOVA Login - Microsoft Internet Explorer provided by Siemens Medical Solutions
File Edit View Tools Help
Back Search Favorites
Address https://smskbqa.medical.siemens.com/selfservice
Go Links

Fig. 46: Selection of the CS Knowledge Base

- Confirm the message window that appears regarding establishment of a “Secure Connection” by clicking on **<OK>**. The network connection will be established.
- Continue with section Login to the CS Knowledge Base.(Login to the CS Knowledge Base / p. 86).

Accessing the CS Knowledge Base from syngo VE31C onwards

NOTE	**The account and password from SCD is used for the new knowledge base, see (Prerequisites / p. 79).**

NOTE	**There is a new link to the KB:** **https://smskbqa.medical.siemens.com/selfservice**

Precondition for Access to the new Knowledge Base

The new CS Knowledge Base is accessible from systems connected via a router (VPN over DSL) to the SRS server.

1. Choosing the “Remote Service Center”

1. Select Local Service --> Configuration
2. Click on “Site Info” in the window.
3. Click on “Next”.

4. In the next window, choose the appropriate Remote Service Center (Europe, Asia or USA), see (1/Fig. 47 / p. 84).

Fig. 47: Remote Service Center

5. Click on “Finish”.

2. Setting the Remote Access Mode to “Limited access” or “Limited access permanent”

Procedure for Access to the Knowledge Base

For access to the KB, the following steps are necessary:

1. Start the syngo service software.
2. Click on (1/Fig. 48 / p. 85).

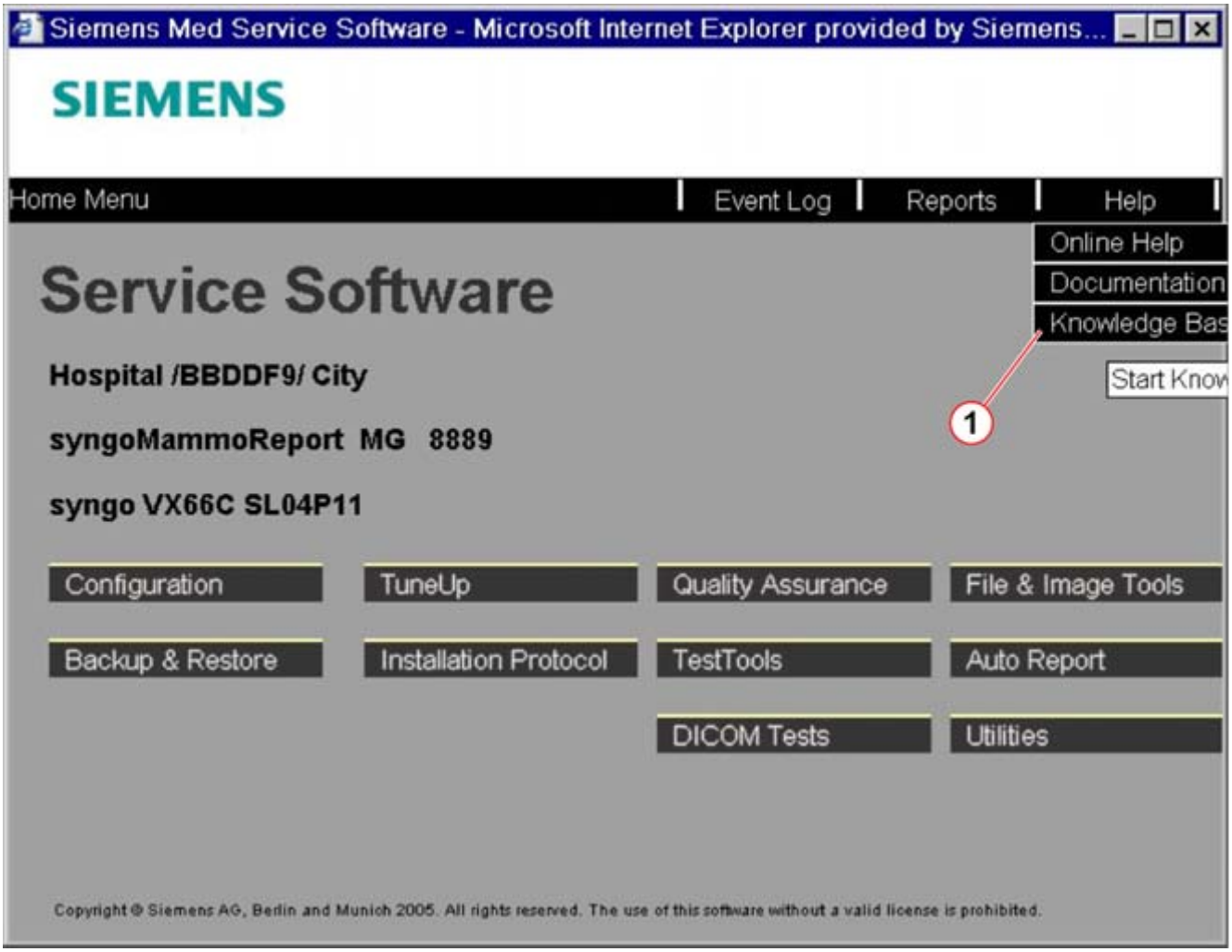

Fig. 48: Starting the knowledge base in syngo

3. Wait >= 10 seconds to open the login mask of the Knowledge Base.

Login to the CS Knowledge Base

- Login in to the Knowledge Base.
  Type in (1/Fig. 49 / p. 86) your e-mail address
  e.g. Frank.Urban@siemens.com
  Type in (2/Fig. 49 / p. 86) the password of the SCD account.
  Click on (3/Fig. 49 / p. 86) to start the login process.

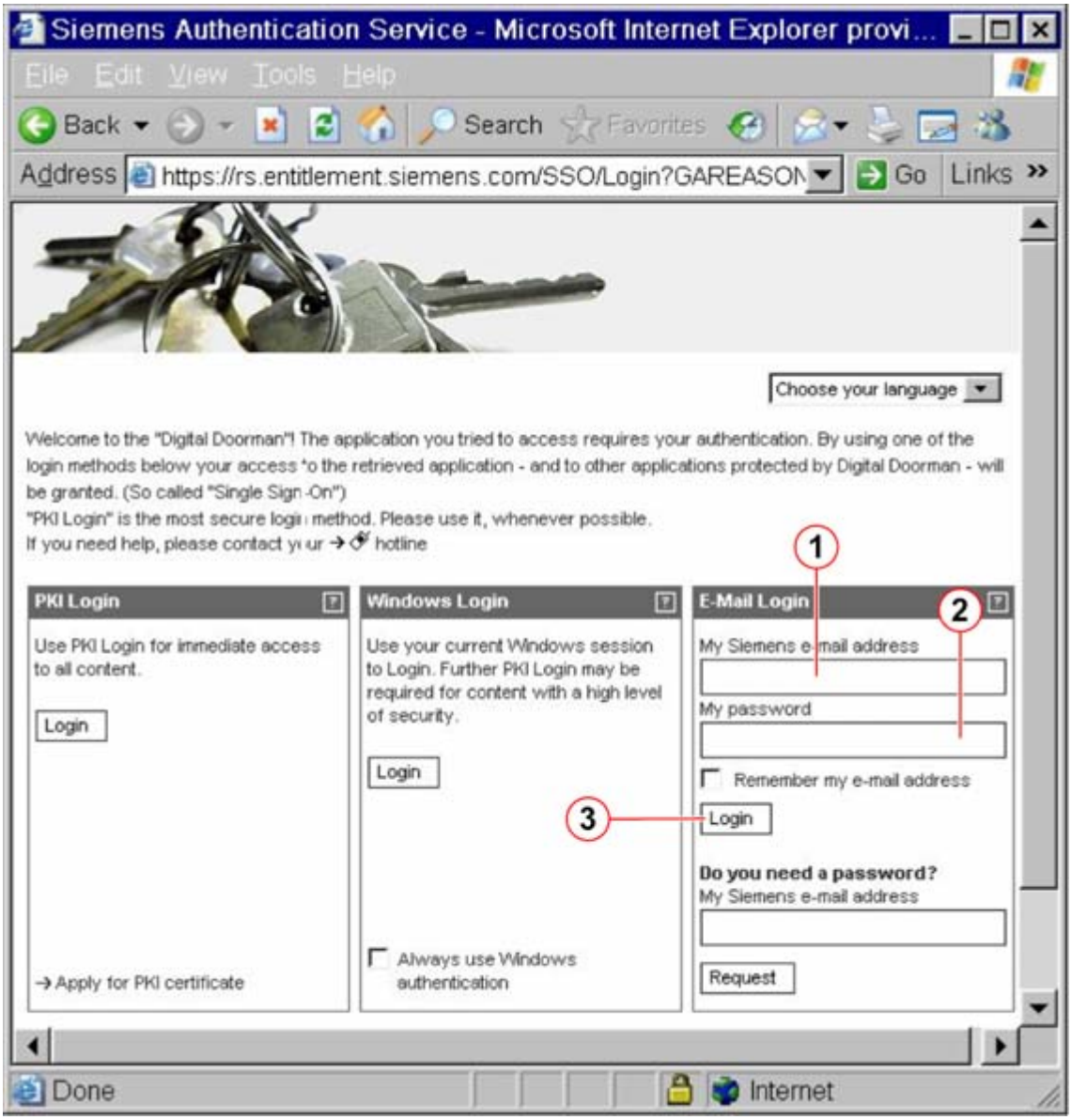
Siemens Authentication Service - Microsoft Internet Explorer provi...
File Edit View Tools Help
Back Search Favorites
Address https://rs.entitlement.siemens.com/SSO/Login?GAREASON
Go Links
Choose your language
Welcome to the "Digital Doorman"! The application you tried to access requires your authentication. By using one of the login methods below your access to the retrieved application - and to other applications protected by Digital Doorman - will be granted. (So called "Single Sign-On")
"PKI Login" is the most secure login method. Please use it, whenever possible.
If you need help, please contact your hotline
1
2
3
PKI Login
Use PKI Login for immediate access to all content.
Login
→ Apply for PKI certificate
Windows Login
Use your current Windows session to Login. Further PKI Login may be required for content with a high level of security.
Login
Always use Windows authentication
E-Mail Login
My Siemens e-mail address
My password
Remember my e-mail address
Login
Do you need a password?
My Siemens e-mail address
Request
Done
Internet

Fig. 49: Knowledge base login screen

➪ The new Knowledge Base mask will be opened.

NOTE

On systems without syngo or syngo lower than VE31C:

Close Internet Explorer to get back to the User UI after ending the Intranet session.

Restore all changes that were made under the point “Settings in Internet Explorer”, i.e., bring the system back to its original status.

Passwords

The only password needed during the SRS configuration is the connection password for access via FTP to the SRS access server (account “rdiagftp”).

The password is listed in the CS Knowledge Base:

Passwords in the CS Knowledge Base

For access to the new KB, see (Knowledge Base / Life Net / p. 79).

Use the new **Search options** to find the password list for your BU.

SRS Access Server

Three worldwide access servers (SRS Portal) make your system accessible to Siemens Remote Service.

Time zone / Server function	I (Europe, Africa) Fuerth	II (America) Newark	III (Asia, Australia) Singapore
SRS Access Server[1]	LUX09505	SRSACC1	SGPT806X
See note	**194.138.39.18**	**129.73.116.92**	**194.138.243.178**

1. This is the target server for the configuration of the FTP transfer functionality in the modality service configuration

NOTE

If the customer uses network configuration with Outside NAT (Outside NAT / p. 20), another IP address for the SRS access server is needed and is assigned by the hospital network administrator.

System Management Server

System management servers are located in the SRS server environment in Europe, Asia and America. Systems report to these servers with statistical quality data and escalate cases involving severe malfunctions of the system.

SRS Backend for MNP Versions VExx and VFxx

Time zone / Server function	**I (Europe, Africa) Fuerth**	**II (America) Newark**	**III (Asia, Australia) Singapore**
HP Openview GUI (event)	LUX09330 **194.138.39.19**	SRSMON1 **129.73.116.91**	SGPT3179X **194.138.243.179**
Event Management **See note**	FTHW9MTA **194.138.39.20**	SRSSQL01 **129.73.116.90**	SGPT3180A **194.138.243.180**
Asset Management **See note**	FTHW9MTA **194.138.39.20**	SRSSQL01 **129.73.116.90**	SGPT3180A **194.138.243.180**
Software distribution (**MNP access server** [1]). **See note**	FTHW9MVA **194.138.39.22**	SRSSQL03 **129.73.116.94**	SGPT3182A **194.138.243.182**

1. This is the target server for installation of the Managed Node Package (MNP)

NOTE

If the customer uses network configuration with Outside NAT, other IP addresses for the system management servers are needed and are assigned by the hospital network administrator.

SRS Backend for MNP Version VGxx

Time zone / Server function	**I (Europe, Africa) Fuerth**	**II (America) Newark**	**III (Asia, Australia) Singapore**
HP Openview GUI (event)	LUX09330 **194.138.39.19**	SRSMON1 **129.73.116.91**	SGPT3179X **194.138.243.179**
Event Management **See note**	LUX09330 **194.138.39.19**	SRSMON1 **129.73.116.91**	SGPT3179X **194.138.243.179**

Time zone / Server function	**I (Europe, Africa) Fuerth**	**II (America) Newark**	**III (Asia, Australia) Singapore**
Asset Management **See note**	LUX09330 **194.138.39.19**	SRSMON1 **129.73.116.91**	SGPT3179X **194.138.243.179**
Software distribution (**MNP access server** [1]). **See note**	FTHW9MUA **194.138.39.21**	SRSSQL02 **129.73.116.93**	SGPT3181A **194.138.243.181**

1. This is the target server for installation of the Managed Node Package (MNP)

NOTE

If the customer uses network configuration with Outside NAT, other IP addresses for the system management servers are needed and are assigned by the hospital network administrator.

Country Codes

Tab. 11 ISO 3166 Country Codes

Afghanistan	AF	Grenada	GD	Russian Federation	RU
Albania	AL	Guadeloupe	GP	Rwanda	RW
Algeria	DZ	Guam	GU	S. Georgia and S. Sandwich Islands	GS
American Samoa	AS	Guatemala	GT	Saint Kitts and Nevis	KN
Andorra	AD	Guinea	GN	Saint Lucia	LC
Angola	AO	Guinea-Bissau	GW	Saint Vincent & the Grenadines	VC
Anguilla	AI	Guyana	GY	Samoa	WS
Antarctica	AQ	Haiti	HT	San Marino	SM
Antigua and Bermuda	AG	Heard and McDonald Islands	HM	Sao Tome and Principe	ST
Argentina	AR	Honduras	HN	Saudi Arabia	SA
Armenia	AM	Hong Kong	HC	Senegal	SN
Aruba	AW	Hungary	HU	Seychelles	SC
Australia	AU	Iceland	BS	Sierra Leone	SL
Austria	AT	India	IN	Singapore	SG
Azerbaijan	AZ	Indonesia	ID	Slovenia	SI
Bahamas	BS	Iran	IR	Slovak Republic	SK
Bahrain	BH	Iraq	IQ	Solomon Islands	SB
Barbados	BB	Ireland	IE	Somalia	SO
Bangladesh	BD	Israel	IL	South Africa	ZA
Belarus	BY	Italy	IT	Spain	ES
Belgium	BE	Jamaica	JM	Sri Lanka	LK
Belize	BZ	Japan	JP	St. Helena	SH
Benin	BJ	Jordan	JO	St. Pierre and Miquelon	PM
Bermuda	BM	Kazakhstan	KZ	Sudan	SD
Bahamas	BS	Kenya	KE	Suriname	SR
Bhutan	BT	Kiribati	KI	Svalbard & Jan Mayen Islands	SJ

Botswana	BW	Korea (North)	KP	Swaziland	SZ
Bolivia	BO	Korea (South)	KR	Sweden	SE
Bosnia and Herzegovina	BA	Kuwait	KW	Switzerland	CH
Bouvet Island	BV	Kyrgyzstan	KG	Syria	SY
Brazil	BR	Laos	LA	Taiwan	TW
British Indian Ocean Territory	IO	Latvia	LV	Tajikistan	TJ
Brunei Darus-salam	BN	Lebanon	LB	Tanzania	TZ
Bulgaria	BG	Liechtenstein	LI	Thailand	TH
Burkina Faso	BF	Liberia	LR	Togo	TG
Burundi	BI	Libya	LY	Tokelau	TK
Cambodia	KH	Lesotho	LS	Tonga	TO
Cameroon	CM	Lithuania	LT	Trinidad and Tobago	TT
Canada	CA	Luxembourg	LU	Tunisia	TN
Cape Verde	CV	Macau	MO	Turkey	TR
Cayman Islands	KY	Madagascar	MG	Turkmenistan	TM
Central African Republic	CF	Malawi	MW	Turks and Caicos Islands	TC
Chad	TD	Malaysia	MY	Tuvalu	TV
Chile	CL	Maldives	MV	Uganda	UG
China	CN	Mali	ML	Ukraine	UA
Christmas Island	CX	Malta	MT	United Arab Emirates	AE
Cocos (Keeling) Islands	CC	Marshall Islands	MH	United King-dom	UK
Colombia	CO	Martinique	MQ	United States	US
Comoros	KM	Mauritania	MR	US Minor Outly-ing Islands	UM
Congo	CG	Mauritius	MU	Uruguay	UY
Congo, Demo-cratic Republic	CD	Mayotte	YT	USSR (former)	SU
Cook Islands	CK	Mexico	MX	Uzbekistan	UZ
Costa Rica	CR	Micronesia	FM	Vanuatu	VU
Cote D'Ivoire (Ivory Coast)	CI	Monaco	MC	Vatican City State (Holy See)	VA

Croatia (Hrvatska)	HR	Moldova	MD	Venezuela	VE
Cuba	CU	Morocco	MA	Vietnam	VN
Cyprus	CY	Mongolia	MN	Virgin Islands (British)	VG
Czech Republic	CZ	Montserrat	MS	Virgin Islands (U.S.)	VI
Denmark	DK	Mozambique	MZ	Wallis and Futuna Islands	WF
Djibouti	DJ	Myanmar	MM	Western Sahara	EH
Dominica	DM	Namibia	NA	Yemen	YE
Dominican Republic	DO	Nauru	NR	Zambia	ZM
East Timor	TP	Nepal	NP	Zimbabwe	ZW
Ecuador	EC	Netherlands	NL		
Egypt	EG	Netherlands Antilles	AN		
El Salvador	SV	Neutral Zone	NT		
Equatorial Guinea	GQ	New Caledonia	NC		
Eritrea	ER	New Zealand (Aotearoa)	NZ		
Estonia	EE	Nicaragua	NI		
Estonia	EE	Niger	NE		
Ethiopia	ET	Nigeria	NG		
Falkland Islands (Malvinas)	FK	Niue	NU		
Faeroe Islands	FO	Norfolk Island	NF		
Fiji	FJ	Northern Mariana Islands	MP		
Finland	FI	Norway	NO		
France	FR	Oman	OM		
France, Metropolitan	FX	Pakistan	PK		
French Guiana	GF	Palau	PW		
French Polynesia	PF	Panama	PA		
French Southern Territories	TF	Papua New Guinea	PG		

F.Y.R.O.M. (Macedonia)	MK	Paraguay	PY
Gabon	GA	Peru	PE
Gambia	GM	Philippines	PH
Georgia	GE	Pitcairn	PN
Germany	DE	Poland	PL
Ghana	GH	Portugal	PT
Gibraltar	GI	Puerto Rico	PR
Great Britain (UK)	GB	Qatar	QA
Greece	GR	Reunion	RE
Greenland	GL	Romania	RO

Chapter	Section	Action
3, 4, 5, 8	All	Added HP information.

A
Adding a static route 19
Auto Transfer 43

B
Basic Ports 40

C
Changing the Computer Name Subsequently13
Changing the IP Address 16
Checking the static route 18
Computer name 13
Computer name restrictions 13
Connectivity Test 22
Country Codes 92
CS Knowledge Base for Systems without syngo or syngo lower than VE31C81
CS Knowledge Base from VE31C onwards83

D
Deleting a static route 18

F
Final Configuration Checklist 77
FTP 41
FTP Test 41

G
Graphics & Screenshots in this Document7

H
Handling the Pre-Connect Tool 31

I
Identification 13
Inside NAT 21
IP Adresse (Local Host) 15

K
Knowledge Base 79

L
Life Net 79

M
Mail 47
Mail Test 47
MNP Connectivity Check 67
MNP Installation Check 66
MNP Installation/Activation of VE/VF Versions50
MNP Installation/Activation of VGxx Version52
MNP Log Files 57
MNP pop-ups 64
MNP TCP/IP Ports 54
MNP Troubleshooting 57
MNP uninstallation 64

N
Network Address Translation (NAT) . . 20
Network Layouts 9
Notes. 7

O
Outside NAT 20

P
Password for FTP 41
Passwords. 88
Ping. 22
Pre-Connect Tool 6
Pre-Connect Tool Download 77

R
RDiag 8, 78
RDiag Server. 41
Remote Service via Corina 38
Remote Update Handling 69
Requirements 6
Router Order Form 77

S
Safety information, general 7
Screenshots & Graphics in this Document7
Siemens Remote Portal 78
Software Distribution. 69
Specify an IP address 15
SRS Access Server. 89
SRS Help Desk 76
SRS Toolkit 77
Static Route. 18
System Management Server. 90

T
Test Ping not Alive. 29
Tools, Test Equipment and Aids 6
tracert 22

V
Virus Protection. 70
Virus Protection, Silent Mode 74
VPN. 12